RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Agence Française Anticorruption

PROJET DE MISE A JOUR DES RECOMMANDATIONS SUR LE REFERENTIEL ANTICORRUPTION APPLICABLE AUX ACTEURS PRIVÉS ASSUJETTIS A L'ARTICLE 17 DE LA LOI n° 2016-1691 DU 9 DECEMBRE 2016 – CONSULTATION NATIONALE
Version du 15 octobre 2020

I. Introduction

1. Aux termes du premier alinéa du 2° de l'article 3 de la loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique (ci-après « la loi »), l'Agence française anticorruption (AFA) « *élabore des recommandations destinées à aider les personnes morales de droit public et de droit privé à prévenir et à détecter les faits de corruption, de trafic d'influence, de concussion, de prise illégale d'intérêt, de détournement de fonds publics et de favoritisme*. »

2. Ces délits, regroupés sous une section du code pénal intitulée « des manquements au devoir de probité »[1], seront indifféremment désignés dans la totalité du présent document, de façon générique, sous les termes « d'atteintes à la probité » ou de « corruption ».

3. Les présentes recommandations visent à faciliter la mise en place par les sociétés et établissements publics industriels et commerciaux assujettis à l'article 17 de la loi, des mesures et procédures destinées à prévenir et détecter les faits de corruption et de trafic d'influence (ci-après dénommé « dispositif anticorruption »). Elles déclinent pour ces entreprises les recommandations générales définies par le référentiel commun (cf. document distinct sur le référentiel commun).

I.1) Portée juridique des recommandations

4. Les recommandations ne créent pas d'obligation juridique à l'égard de ceux auxquels elles s'adressent.

5. D'autres méthodologies peuvent être employées sous réserve que leur mise en œuvre permette d'atteindre un même résultat.

6. Les recommandations sont opposables à l'AFA, qui s'y réfère dans le cadre de ses missions de conseil et de contrôle.

I.2) Déclinaison des recommandations par les entreprises en fonction de leur propre profil de risques

7. Chaque entreprise applique les présentes recommandations suivant son profil de risques, qui varie en fonction de différents paramètres, notamment les types de biens ou services qu'elle produit ou fournit, sa structure de gouvernance, sa taille, son secteur d'activité, ses implantations géographiques et les différentes catégories de tiers avec lesquels elle interagit.

8. Les entreprises qui exercent un contrôle de droit ou de fait sur d'autres entités (par exemple : filiales, succursales, agences) sont invitées à mettre en place des procédures et un contrôle interne, visant à s'assurer de la qualité et de l'efficacité du dispositif anticorruption dans l'ensemble du périmètre qu'elles contrôlent.

9. L'organisation et les procédures définies sont déclinées par les différentes entités en tenant compte de leurs spécificités et des risques de corruption et de trafic d'influence auxquelles elles sont exposées.

[1] À l'exception de la corruption privée (articles 445-1 à 445-2 du code pénal).

II. La mise en œuvre du référentiel anticorruption

10. En application du I de l'article 17 de la loi n° 2016-1691 du 9 décembre 2016, les dirigeants de certaines entreprises sont personnellement tenus de « *prendre les mesures et procédures destinées à prévenir et détecter la commission, en France ou à l'étranger, des faits de corruption et de trafic d'influence* ».

11. Les mesures et procédures énumérées au II de l'article 17 ne visent donc qu'à la prévention des deux des six infractions énumérées par l'article 1 de la loi, la corruption et le trafic d'influence. Au regard de ces dispositions, la prévention et la détection de ces deux infractions peuvent être envisagées par la mise en œuvre de mesures et procédures identiques puisque ces délits recouvrent strictement les mêmes réalités en termes d'éléments matériels constitutifs et ne se distinguent, dans leur aspect passif, que par la qualité de leur auteur. Ces faits seront génériquement qualifiés de « corruption » dans la suite de cette recommandation.

12. Les mesures et procédures ne sont pas obligatoires pour les sociétés et EPIC, dont le chiffre d'affaires et le nombre de salariés sont inférieurs aux seuils précités. Il leur est toutefois recommandé de s'engager dans le déploiement d'un dispositif répondant aux mêmes objectifs.

13. Il est également rappelé que les sociétés d'économie mixte et les établissements publics industriels et commerciaux qui atteignent les seuils définis à l'article 17 de la loi n° 2016-1691 du 9 décembre 2016 sont en outre assujettis aux obligations définies par le 3° de l'article 3 de la loi.

14. Une entreprise assujettie, qui met correctement en œuvre la méthodologie préconisée par l'AFA dans ses recommandations, bénéficie d'une présomption simple de conformité.

15. En revanche, une entreprise qui fait le choix de ne pas suivre la méthode préconisée par l'AFA dans ses recommandations doit démontrer la pertinence, la qualité et l'effectivité du dispositif de détection et de prévention de la corruption en justifiant de la validité de la méthode qu'elle a librement choisie et suivie.

16. Les présentes recommandations déclinent pour les entreprises soumises à l'article 17 de la loi, le référentiel anticorruption qui repose sur trois piliers indissociables : l'engagement de l'instance dirigeante, la connaissance des risques de corruption à travers une cartographie des risques et la gestion de ces risques par la mise en œuvre de mesures de prévention, de détection et de remédiation.

II.1) L'engagement de l'instance dirigeante

17. Conformément au I de l'article 17 de la loi, les instances dirigeantes *« (…) sont tenues de prendre les mesures destinées à prévenir et détecter la commission, en France ou à l'étranger, de faits de corruption ou de trafic d'influence selon les modalités prévues au II ».*

18. À défaut, leur responsabilité peut être engagée devant la commission des sanctions de l'AFA. Il est donc dans leur intérêt de veiller à la mise en œuvre d'un dispositif anticorruption adapté sur l'ensemble du périmètre d'intervention de l'entreprise.

1. Définition et responsabilité de l'instance dirigeante

19. Constituent l'instance dirigeante les personnes suivantes :

- les présidents, les directeurs généraux et les gérants de société ayant leur siège social en France, employant au moins cinq cents salariés et dont le chiffre d'affaires est supérieur à 100 millions d'euros ;
- les présidents, des directeurs généraux et des gérants de société appartenant à un groupe de

sociétés dont la société mère a son siège social en France, dont l'effectif comprend au moins cinq cents salariés et dont le chiffre d'affaires consolidé est supérieur à 100 millions d'euros ;

- les présidents et directeurs généraux d'établissements publics à caractère industriel et commercial employant au moins cinq cents salariés, ou appartenant à un groupe public dont l'effectif comprend au moins cinq cents salariés, et dont le chiffre d'affaires ou le chiffre d'affaires consolidé est supérieur à 100 millions d'euros ;
- les membres du directoire des sociétés anonymes régies par l'article L. 225-57 du code de commerce et employant au moins cinq cents salariés, ou appartenant à un groupe de sociétés dont l'effectif comprend au moins cinq cents salariés, et dont le chiffre d'affaires ou le chiffre d'affaires consolidé est supérieur à 100 millions d'euros.

20. Si les membres des conseils d'administration ou des conseils de surveillance ne sont pas visés par cette définition, ils s'assurent, dans le cadre de leur mission de surveillance des activités de l'entreprise, de la pertinence et de l'efficacité des mesures prises par les dirigeants afin de se conformer aux obligations légales. Dans les sociétés à conseil d'administration, l'AFA recommande que le dispositif anticorruption et ses actualisations périodiques soient validés par le conseil d'administration.

2. Responsabilité de l'instance dirigeante

21. L'instance dirigeante s'engage à mettre en œuvre une politique de tolérance zéro envers tout fait de corruption, promeut et diffuse la culture de la conformité anticorruption au sein de l'entreprise et vis-à-vis des tiers, en érigeant la prévention et la détection des faits de corruption à un niveau prioritaire. Ceci constitue un élément fondateur de la démarche de prévention et de détection.

22. La responsabilité de la mise en place du dispositif anticorruption incombe à l'instance dirigeante qui peut, le cas échéant, en déléguer la mise en œuvre opérationnelle à une personne dénommée, dans la suite du présent document, « responsable de la fonction conformité ».

23. L'instance dirigeante définit la stratégie de gestion des risques et s'assure de la mise en œuvre et de l'efficacité du dispositif anticorruption. À cet égard, elle veille à formaliser l'approbation du dispositif et en particulier de la cartographie. Elle s'assure de la mise en place d'un plan d'actions y afférent et des moyens adaptés pour l'exécuter et pour en assurer le suivi régulier. Par ailleurs, les sociétés qui sont soumises aux dispositions des articles L. 225-37 6^{e} alinéa ou L. 225-68 7^{e} alinéa du code de commerce incluent dans leur rapport un développement spécifique sur leur dispositif anticorruption. L'instance dirigeante vérifie, au moyen d'indicateurs et de rapports de contrôle et d'audit, que le dispositif anticorruption est organisé, efficace et à jour.

24. Au-delà de la mise en œuvre des mesures et procédures qui composent le dispositif anticorruption, l'instance dirigeante est invitée à intégrer des mesures anticorruption aux procédures et politiques de l'entreprise à risque.

25. En matière de gestion des ressources humaines, l'instance dirigeante s'assure que :

- le processus de recrutement et de nomination des cadres et des personnels les plus exposés inclut la vérification de l'attachement à l'éthique des affaires ;
- le respect des mesures de prévention de la corruption est pris en compte dans la fixation de leurs objectifs annuels et l'évaluation de leur performance. Les initiatives des managers pour promouvoir la prévention et la détection de faits de corruption auprès de leurs équipes doivent être valorisées.

26. En matière de politique commerciale, l'instance dirigeante s'assure que la politique d'octroi des remises commerciales, rabais et ristournes ne peut pas donner lieu à des pratiques corruptives.

27. L'instance dirigeante met en place un régime disciplinaire et applique des sanctions adéquates en cas de faits de corruption.

3. Moyens dédiés

28. La mise en œuvre d'un dispositif anticorruption nécessite des moyens humains et financiers proportionnés au profil de risque de l'entreprise.

29. Ces moyens doivent couvrir notamment :

- l'équipe dédiée à la conformité anticorruption ;
- le recours éventuels à des conseils ou prestataires externes ;
- la mise en place d'outils informatiques tels que des outils d'évaluation de l'intégrité des tiers, d'alerte interne, de gestion des risques, de monitoring, d'e-learning, etc. ;
- la gestion de la formation anticorruption ;
- la production de rapports et d'évaluations périodiques.

Le responsable de la fonction conformité anticorruption

30. La désignation du responsable de la fonction conformité peut faire l'objet d'une communication spécifique à l'ensemble des personnels et être formalisée par une lettre de mission de l'instance dirigeante précisant :

  - les missions confiées ;
  - les éléments qui garantissent l'indépendance de la fonction conformité à travers son positionnement dans l'organigramme et les modalités d'accès à l'instance dirigeante, au conseil d'administration et aux comités spécialisés qui en émanent ;
  - l'articulation avec les autres fonctions de l'entreprise et les autres domaines de la conformité ;
  - l'organisation de la fonction conformité dans l'entreprise, notamment les moyens matériels et humains qui y sont consacrés.

31. L'instance dirigeante s'assure que le responsable de la fonction conformité dispose des moyens lui permettant de réaliser ses missions, de coordonner les fonctions concernées et de lui rendre compte.

32. Dans le cas d'une entreprise structurée autour d'une entité centrale de type maison-mère et filiales, il est recommandé de nommer un responsable de la fonction conformité au niveau central.

33. Ce responsable peut inciter à la mise en œuvre du dispositif anticorruption dans les filiales, et les assister dans cet exercice, au moyen notamment de la diffusion d'organisations cibles ou de méthodologies et politiques communes. Son action prend en compte les particularités des filiales concernées (taille, risques propres identifiés, options retenues dans l'organisation de la fonction conformité…).

34. Ce responsable de la fonction conformité peut constituer avec ses interlocuteurs conformité de l'entreprise un réseau conformité anticorruption, afin d'aider à la conception, au déploiement et au contrôle de l'entier dispositif. Ce réseau, qui facilite notamment la remontée de questions et d'alertes ainsi que les retours d'expérience, participe à l'amélioration du dispositif global.

35. Le positionnement du responsable de la fonction conformité dans l'entreprise doit lui garantir :

- un accès à toute information utile lui permettant de disposer d'une image fidèle de l'activité

de l'entreprise ;
- l'objectivité de ses appréciations ;
- l'indépendance de son action vis-à-vis des autres fonctions de l'entreprise et la capacité à influer réellement sur ces dernières ;
- un accès aisé à l'instance dirigeante, afin d'en obtenir l'écoute et le soutien.

36. Indépendamment de son positionnement dans l'organigramme, il est primordial que le responsable de la fonction conformité entretienne un lien direct et régulier avec l'instance dirigeante ainsi qu'avec le conseil d'administration ou ses comités spécialisés s'ils existent.

37. Au-delà de ses missions récurrentes, le responsable de la fonction conformité doit être associé aux prises de décisions structurantes pour l'entreprise à la mise en œuvre des projets stratégiques, tels que, par exemple, les fusions-acquisitions, les investissements majeurs ou la prospection de nouveaux marchés, la constitution d'un partenariat, la commercialisation de nouveaux produits.

38. L'indépendance du responsable de la fonction conformité ne signifie pas pour autant l'absence de contrôle. À cet effet, il rend compte à l'instance dirigeante de son activité, qui relève d'ailleurs du périmètre couvert par l'audit interne.

39. L'instance dirigeante s'assure que le responsable de la fonction conformité anticorruption dispose des compétences requises, notamment :

- de la capacité d'exercer une fonction par nature transverse, qui requiert un sens des relations et des compétences en pilotage de projets ;
- d'une connaissance des réglementations liées à la conformité anticorruption, ainsi que des activités de l'entreprise et des techniques de gestion des risques. Cette connaissance peut avoir été acquise par le suivi de formations ou résulter de l'expérience professionnelle.

40. Le périmètre des missions du responsable de la fonction conformité est précisé par l'instance dirigeante en fonction des choix organisationnels et stratégiques retenus ainsi qu'au regard des caractéristiques de l'entreprise (modèle économique, secteur d'activité, taille, etc.). Ce périmètre peut ainsi être étendu à d'autres fonctions ou domaines de la conformité.

41. Afin que son action soit efficace, la fonction conformité anticorruption doit être articulée avec les autres fonctions et activités de l'entreprise.

Une politique de communication interne et externe adaptée

42. L'entreprise communique sur sa politique de prévention et de détection de la corruption, ainsi que sur le dispositif anticorruption qui la matérialise, auprès de l'ensemble du personnel et, afin de dissuader les sollicitations indues, des partenaires extérieurs.

43. Adaptée à sa structure et à ses activités, cette communication porte nécessairement sur le code de conduite, la formation anticorruption et le dispositif d'alerte interne.

II.2) La mise en place d'un dispositif d'évaluation des risques à travers la cartographie des risques de corruption

45. Aux termes du 3° du II de l'article 17 de la loi la cartographie des risques de corruption « *[prend] la forme d'une documentation régulièrement actualisée et destinée à identifier, analyser et hiérarchiser les risques d'exposition de la société à des sollicitations externes aux fins de corruption, en fonction notamment des secteurs d'activité et des zones géographiques dans lesquels la société exerce son activité.* »

46. La lecture combinée des différentes dispositions de l'article 17 et notamment de son I, implique que les entreprises qui y sont soumises doivent réaliser une cartographie couvrant non seulement les risques de corruption comme le précise le texte, mais également ceux de trafic d'influence. Une autre interprétation, qui procéderait d'une lecture littérale du seul 3° de son II, priverait le dispositif global de son efficacité puisque les autres mesures, qui toutes procèdent de cette cartographie, prévoient implicitement (code de conduite, procédures de contrôle comptable, dispositif de formation) ou explicitement (dispositif d'alerte, procédures d'évaluation des tiers…) qu'elles ont aussi pour objet de prévenir et de détecter le trafic d'influence.

47. Au-delà de ce que prévoit le texte, il est recommandé que l'exercice tendant à l'établissement et à la mise à jour de cette cartographie permette d'appréhender les autres risques d'atteinte à la probité (comme le recel de favoritisme) afin d'en faciliter la gestion.

48. Indispensable instrument de la connaissance des risques de corruption, la cartographie permet aux entreprises d'engager et de formaliser une réflexion en profondeur et de créer les conditions d'une meilleure maîtrise de ces risques. Elle est mise en œuvre dans l'objectif de se prémunir contre les conséquences réputationnelles, juridiques, humaines, économiques et financières que pourrait générer leur réalisation.

49. L'établissement de la cartographie des risques de corruption nécessite :

- de disposer d'une connaissance précise de l'entreprise et de ses activités, dont les processus[2] managériaux, opérationnels et support que ces activités nécessitent de mettre en œuvre. Cette connaissance est la condition préalable à l'analyse fine des processus qui garantit que la cartographie des risques de corruption reflète fidèlement les risques auxquels l'entreprise est réellement exposée. Chaque entreprise établit sa propre cartographie des risques de corruption, qui lui est spécifique, et ne peut en conséquence être transposée en l'état à une autre entreprise.
- d'identifier les rôles et responsabilités des acteurs concernés à tous les niveaux de l'entreprise.

1. Objectifs de la cartographie des risques de corruption

50. La cartographie des risques procède d'une analyse objective, structurée et documentée des risques de corruption auxquels une entreprise est exposée dans le cadre de ses activités. Elle résulte de l'analyse de l'ensemble des processus de l'entreprise qui la conduisent à interagir avec les tiers, ainsi que de l'identification des risques de corruption, et ce à chaque stade de ces processus.

51. Elle donne à l'instance dirigeante la visibilité nécessaire pour la mise en œuvre de mesures de prévention et de détection efficaces, proportionnées aux enjeux qu'elle a permis d'identifier et adaptées aux activités de l'entreprise concernée.

52. Deuxième pilier du dispositif anticorruption, la cartographie des risques de corruption permet à l'entreprise de gérer efficacement ses risques à travers les mesures et procédures de prévention, de détection et de remédiation développées ci-dessous. Réciproquement, les enseignements tirés de la mise en

[2] Dans le cadre des présentes recommandations, la notion de processus s'entend d'un ensemble de tâches corrélées ou en interaction qui visent à la satisfaction d'un besoin managérial, opérationnel ou support.

œuvre de ces mesures et procédures sont pris en compte pour établir et mettre à jour la cartographie des risques de corruption. L'ensemble de ces interactions s'inscrit ainsi dans une approche systémique de la cartographie des risques de corruption et des mesures et procédures conçues et mises en œuvre pour les gérer.

2. Caractéristiques de la cartographie des risques de corruption

53. La cartographie des risques est complète dans la mesure où :

- d'une part, elle couvre « de bout en bout » les processus managériaux, opérationnels et support mis en œuvre par les entreprises dans le cadre de leurs activités. Elle appréhende les risques de corruption en prenant en compte les particularités de chaque entreprise : secteurs d'activité, zones géographiques, contexte concurrentiel et réglementaire, typologies de tiers, modèle de revenus, chaîne de valeur, métiers et processus, entreprise interne de l'entreprise, circuits de décision, etc. ;
- d'autre part, elle couvre le périmètre d'intervention de l'entreprise. Ainsi, lorsque l'entreprise exerce un contrôle de droit ou de fait sur d'autres entités, à l'instar d'une maison mère sur ses filiales, elle établit sa cartographie en prenant en compte les risques inhérents aux activités des entreprises contrôlées, après s'être par exemple fait communiquer leurs cartographies. Celles-ci pourront en outre utilement être consolidées au sein de la cartographie des risques de corruption de l'entreprise mère.

54. La cartographie des risques de corruption est formalisée, c'est-à-dire qu'elle prend la forme d'une documentation écrite, structurée et auditable. La forme de la cartographie des risques doit permettre d'en faire un outil de pilotage des risques et faciliter également l'appréciation interne (par l'audit notamment) et externe (en cas de contrôle administratif ou de procédure judiciaire) de la pertinence du dispositif anticorruption.

55. Au choix de l'entreprise, la documentation peut être organisée, par exemple, par métier, par processus, par entité ou par zone géographique. Elle est accompagnée d'une annexe décrivant notamment les rôles et responsabilités dans son élaboration, les modalités et les méthodologies mises en œuvre pour identifier, évaluer, hiérarchiser et gérer les risques de corruption.

56. La cartographie des risques est évolutive eu égard à la nécessité de réévaluer les risques de manière périodique, en particulier chaque fois qu'une évolution notable se produit dans l'entreprise. À la faveur de son actualisation, la cartographie participe d'un processus d'amélioration continue permettant aux entreprises de renforcer la maîtrise de leurs risques.

3. Les différentes étapes de mise en place d'une cartographie des risques corruption

57. La cartographie des risques de corruption procède d'une analyse objective, structurée et documentée des risques de corruption auxquels une entreprise est exposée dans le cadre de ses activités. La description fait ressortir l'impact des risques (gravité) et leur probabilité d'occurrence (fréquence), les éléments susceptibles de les accroître (facteurs aggravants) ainsi que les réponses apportées dans le cadre du dispositif de maîtrise des risques existant ou à apporter dans le cadre d'un plan d'actions.

58. Dans ce contexte, afin d'identifier, d'évaluer et de gérer les risques de corruption, il est recommandé de respecter les étapes ci-après, ou d'employer une autre méthode conduisant à une efficacité et pertinence au moins similaires.

59. Pour les entreprises ayant déjà conduit des travaux de cartographie des risques, par exemple des risques opérationnels, en matière de prévention de la fraude, des risques de blanchiment et du financement du

terrorisme, de prévention des risques environnementaux, ces démarches préexistantes peuvent être capitalisées, sous réserve que la méthode employée pour les construire soit conforme aux préconisations qui suivent.

1ère étape : Rôles et responsabilités des parties prenantes à la cartographie des risques de corruption

60. Au sein des entreprises, les rôles et responsabilités sont répartis comme suit :

- l'instance dirigeante promeut l'exercice de cartographie des risques et donne les moyens de sa mise en œuvre au responsable de la fonction conformité.

  Elle valide la stratégie de gestion des risques mise en œuvre sur son fondement et s'assure de la mise en œuvre du plan d'actions retenu.

- le responsable de la fonction conformité coordonne l'élaboration de la cartographie des risques, en accompagnant l'entreprise dans le recensement des processus, dans l'identification des risques de corruption, dans l'évaluation et la hiérarchisation de ces risques et dans la définition et la mise en œuvre de mesures concourant à leur maîtrise.

  Le responsable de la fonction conformité communique à l'instance dirigeante la cartographie des risques à chacune de ses mises à jour ainsi que le suivi du plan d'actions.

- les responsables des processus décisionnels, opérationnels, comptables et support contribuent à l'élaboration et à la mise à jour de la cartographie des risques. Ils rendent compte des risques spécifiques au périmètre relevant de leur responsabilité afin qu'en soient tirées les conséquences sur l'identification, l'évaluation et la hiérarchisation des risques.

- le responsable en charge de la maîtrise des risques, quand l'entreprise possède une telle fonction, contribue également à la définition de la méthodologie utilisée pour identifier, analyser, hiérarchiser et gérer les risques de corruption. Sur ce point, le responsable de la fonction conformité et le responsable de la gestion des risques travaillent en étroite collaboration. La cartographie des risques de corruption peut être réalisée en même temps qu'une cartographie concernant d'autres risques (opérationnels, comptables, de fraude,…) afin d'optimiser les ressources mobilisées. Il est alors important de bien distinguer, dans l'exercice de cartographie, entre les risques de corruption et les autres.

- les personnels, forts de leur expérience pratique des processus de l'entreprise, apportent leur contribution à l'exercice de cartographie en rendant compte des facteurs spécifiques aux fonctions exercées et aux risques encourus afin qu'en soient tirées les conséquences sur l'identification, l'évaluation et la hiérarchisation des risques.

61. L'entreprise, lors de l'élaboration de sa cartographie, veille à appréhender les risques inhérents aux activités exercées par l'ensemble des personnels travaillant dans la structure, quel que soit leur statut, ainsi qu'aux dirigeants, aux administrateurs et aux gérants.

2e étape : Identification des risques inhérents aux activités de l'entreprise (recensement des processus et scénarios de risques)

62. L'identification des risques de l'entreprise s'appuie sur une analyse fine de ses processus. Dans une première étape, l'entreprise pourra établir un recensement de ces processus, le cas échéant sur le fondement d'une cartographie des processus préexistante. Lors de ce premier recensement, l'entreprise s'attache à ne

pas préjuger des résultats de la cartographie des risques en dressant a priori une liste de processus jugés les plus représentatifs ou les plus exposés aux risques.

63. Sur la base du recensement des processus, l'entreprise organise des ateliers collectifs avec des personnels de tous niveaux hiérarchiques et issus de toutes les fonctions de l'entreprise choisis pour leur maîtrise de la mise en œuvre opérationnelle de ces processus. Elle s'assure, au besoin par des ateliers organisés au niveau pertinent, que les spécificités des différents métiers, filiales ou zones géographiques au sein desquels elle déploie ses activités sont prises en compte. Ces ateliers permettent la libre expression des participants et font l'objet de comptes rendus écrits.

64. Ces ateliers ont pour objet d'identifier, par processus, des scénarios de risques auxquels l'entreprise est exposée dans le cadre de ses activités, le cas échéant attachés à certains métiers, filiales ou zones géographiques. Il ne s'agit pas de décliner la typologie théorique des risques auxquels l'entreprise est exposée, mais de procéder à un état des lieux précis permettant d'identifier, de manière circonstanciée et documentée, les scénarios de risques qui lui sont propres. Si une liste de risques pré établie peut constituer un des supports sur lesquels peut s'appuyer la réflexion menée lors de ces entretiens, elle ne saurait pré déterminer la nature, le nombre et la classification des scénarios de risque retenus à l'issue des entretiens : l'entreprise doit en effet fonder sa cartographie sur la réalité de ses processus.

65. La cartographie des risques intègre l'intervention des tiers de l'entreprise, qui peut présenter un risque d'exposition à une sollicitation aux fins de corruption (facteur de risque). Afin de prévenir le risque de sollicitation externe, l'entreprise met par ailleurs en œuvre des procédures d'évaluation des tiers adaptées au niveau de risque (« due diligences »).

66. Les scénarios de risques sont identifiés en tenant compte notamment des facteurs de risque suivants :

- Pays,
- Secteurs d'activité ;
- Nature des opérations, notamment les d'opérations stratégiques (opérations de fusions-acquisitions, cessions d'actifs, association avec un nouveau partenaire stratégique…) ;
- Personnels ;
- Nature du tiers, secteur d'activité du tiers, relation directe ou indirecte, présence d'une personne politiquement exposée, dépendance économique ;
- Durée du cycle de vente et pression concurrentielle, modalités d'objectivation des commerciaux ;
- Conditions de paiement ;
- Historique des incidents : doivent notamment être pris en compte les incidents ayant affecté l'entreprise, tels que ses audits internes ou son dispositif d'alerte interne ont permis de les révéler, les faits ayant donné lieu à l'application du régime disciplinaire et à des décisions juridictionnelles concernant des entreprises similaires.

3e étape : Évaluation des risques bruts

67. Cette étape vise à évaluer le niveau de vulnérabilité de l'entreprise pour chaque scénario de risque identifié à l'étape précédente. Il s'agit ici d'identifier les risques « bruts » auxquels l'entreprise est exposée, c'est-à-dire les risques considérés en amont des moyens de maîtrise mis en œuvre.

68. Ce niveau de vulnérabilité est évalué au moyen des trois indicateurs suivants : l'impact, la fréquence et les facteurs aggravants.

69. Une analyse de l'impact de chaque scénario de risque identifié est menée. Cet impact peut être réputationnel, financier, économique ou juridique. Un même scénario de risque peut cumuler plusieurs types d'impacts.

70. Une probabilité d'occurrence est déterminée à l'aide des informations les plus complètes et les plus adaptées à la spécificité du risque identifié (exemple : historique des incidents).

71. L'appréciation des facteurs jugés aggravants est réalisée par l'application de coefficients de gravité. Par exemple, dans la situation des entreprises développant leurs activités à l'international, ce coefficient permet de prendre en compte, au stade de l'évaluation des risques bruts, l'incidence de l'implantation géographique.

72. Les ateliers organisés pour identifier les risques peuvent utilement procéder à l'évaluation des risques bruts identifiés. Qu'elle s'appuie ou pas sur ces ateliers, l'évaluation des risques bruts est conduite sur le fondement d'une méthodologie homogène : l'entreprise veille notamment à ce que les évaluations des risques bruts émanant des différents métiers, filiales ou zones géographiques puissent être agrégées de manière cohérente.

4e étape : Évaluation des risques nets ou résiduels

73. Cette étape vise à évaluer le niveau de maîtrise des risques par l'entreprise afin de déterminer les risques « nets » ou « résiduels » auxquels elle est exposée. Il s'agit donc de réévaluer les scénarios de risques « bruts » en prenant en considération les moyens de maîtrise des risques déjà existants et mis en œuvre.

74. Il convient dès lors, à ce stade d'élaboration de la cartographie, d'évaluer l'efficacité des mesures de maîtrise des risques existantes, comme celles inhérentes à l'existence de procédures formalisées, de dispositifs de formation et aux contrôles internes, en s'appuyant notamment sur les audits réalisés.

75. Idéalement, l'évaluation des risques nets ou résiduels est faite par le responsable de la fonction conformité, avec l'appui éventuel de l'audit interne et du responsable en charge de la maîtrise des risques quand l'entreprise possède une telle fonction.

5e étape : Hiérarchisation des risques nets ou résiduels et élaboration du plan d'actions

76. Une fois les risques « nets » ou « résiduels » évalués, un classement par niveau des scénarios de risques peut être spontanément établi.

77. Lorsque ces scénarios de risques présentent une évaluation nette de même niveau, il convient de les hiérarchiser au moyen d'une méthodologie objective adaptée aux activités spécifiques de l'entreprise, reposant sur la combinaison de plusieurs critères comme le risque-pays, le chiffre d'affaires, la nature et le type de relations avec les tiers.

78. Cette hiérarchisation des risques permet également de distinguer les scénarios de risques pour lesquels le niveau de maîtrise est considéré comme suffisant de ceux pour lesquels l'instance dirigeante souhaite améliorer la maîtrise du risque, au moyen notamment d'un renforcement du contrôle interne.

79. Une fois cette limite d'acceptabilité fixée et documentée, il s'agit de déterminer, dans le cadre de la stratégie de gestion des risques, les mesures à mettre en œuvre afin de les maîtriser.

80. Sur la base de ces éléments, un plan d'actions est élaboré. Le calendrier et les modalités de mise en œuvre de ce plan d'actions, ainsi que son suivi et les modalités de compte rendu associés, sont confiés à la responsabilité d'acteurs précisément désignés. L'établissement, la formalisation et le suivi de ce plan d'actions constitue une condition de l'efficacité de la cartographie des risques.

6e étape : Formalisation, mise à jour et archivage de la cartographie des risques corruption

81. L'ensemble des éléments précités constitue la cartographie des risques. Sa présentation participe de son appropriation comme outil de pilotage des risques de corruption. Elle peut être, au choix de l'entreprise, organisée par métier, par processus, par entité ou par zone géographique. Elle est accompagnée d'une annexe décrivant les modalités de son élaboration et la méthodologie d'identification, d'évaluation, de hiérarchisation et de gestion des risques.

82. La nécessité éventuelle d'actualiser la cartographie est appréciée chaque année.

83. Cette mise à jour de la cartographie doit suivre la même méthode que celle empruntée pour sa construction dès lors qu'elle offre, au regard des modalités et méthodologies d'identification, d'évaluation, de hiérarchisation et de gestion des risques qu'elle prévoit, l'assurance raisonnable qu'elle reflète fidèlement les risques réels auxquels l'entreprise est exposée.

84. Les éléments suivants qui permettent d'apprécier la mise en œuvre effective de la cartographie doivent être conservés :

- la trace des ateliers (calendriers, notes, comptes rendus) ;
- la méthodologie de calcul des risques « *bruts* », ainsi que les définitions retenues. Les procédures d'identification et de classification des risques adoptées peuvent également être annexées ;
- la méthodologie de calcul des risques « *nets* » ou « *résiduels* » ainsi que les définitions retenues. Les procédures d'identification et de classification des risques adoptées peuvent également être annexées ;
- Les différentes versions des cartographies présentées aux instances dirigeantes, leur validation et les plans d'actions validés y afférents ;
- Les comptes rendus des différents comités dédiés.

85. Les différentes versions des cartographies, ainsi que leur piste d'audit, sont datées, référencées et archivées.

II.3) Prévention des risques de corruption

1. Code de conduite

86. Le 1° du II de l'article 17 de la loi dispose que les personnes mentionnées au I mettent en œuvre « *un code de conduite définissant et illustrant les différents types de comportements à proscrire comme étant susceptibles de caractériser des faits de corruption ou de trafic d'influence. Ce code de conduite est intégré au règlement intérieur de l'entreprise et fait l'objet, à ce titre, de la procédure de consultation des représentants du personnel prévue à l'article L.1321-4 du code du travail.* »

- **Définition et objectifs**

87. Le code de conduite anticorruption, quelle que soit la dénomination qui lui est donnée par l'entreprise, est un document qui manifeste la décision de l'instance dirigeante d'engager l'entreprise dans une démarche de prévention et de détection des faits de corruption

88. Il recueille les engagements et principes de l'entreprise en cette matière. Il définit et illustre les différents types de comportements à proscrire comme étant susceptibles de caractériser des faits de corruption ou de trafic d'influence.

- **Champ d'application**

89. Le code de conduite est applicable à l'ensemble des personnels de l'entreprise.

90. En tant qu'instrument de bonne gouvernance, le code de conduite est applicable partout où l'entreprise exerce une activité, y compris à l'étranger. Il peut être commun à l'ensemble des entités d'une même entreprise à la condition que ce choix n'entrave pas son efficacité. Lorsque l'entreprise exerce une activité à l'étranger, il est recommandé d'y prévoir une déclinaison du code de conduite tenant compte, le cas échéant, des spécificités juridiques locales, pouvant parfois se matérialiser par l'application de normes anticorruption différentes. De même, lorsque l'entreprise exerce des activités sensiblement différentes avec des risques de corruption spécifiques, il peut être opportun pour l'entreprise de décliner son code de conduite au niveau de ses entités.

91. Concernant les autres collaborateurs amenés à travailler avec l'entreprise (sous-traitants, consultants, personnels intérimaires, stagiaires), il est recommandé que le code leur soit communiqué et leur soit rendu opposable, dans le respect des dispositions légales applicables.

- **Processus d'élaboration et de validation**

92. Afin de manifester son engagement, l'instance dirigeante promeut le code de conduite et en applique scrupuleusement les principes. L'exemplarité de l'instance dirigeante est essentielle à la bonne application du code de conduite par les personnels.

93. Si le code de conduite est préparé conjointement par le responsable de la fonction conformité et les personnes qualifiées de l'entreprise, son portage par l'instance dirigeante est déterminant en ce qu'il participe de son appropriation par l'ensemble des collaborateurs. Il favorise ainsi au sein de l'entreprise le développement d'une culture de la conformité, de l'éthique, de l'intégrité et de la probité, dont chacun peut se prévaloir dans sa relation professionnelle.

- **L'interdépendance du code de conduite avec d'autres documents**

94. Le code de conduite peut renvoyer à des fiches « opérationnelles » (ou « processus », ou « procédures » relatives à la politique cadeau ou la gestion des conflits d'intérêts par exemple) qui, sans faire partie du code lui-même, définissent, sur la base de la cartographie des risques, le détail opérationnel des comportements à respecter afin de maîtriser les situations à risque. Il importe que l'ensemble de ces documents constituent un ensemble cohérent, clairement articulé et dont la lisibilité et l'accessibilité soient assurées pour l'ensemble des collaborateurs.

95. Le code de conduite n'est pas limité à un recueil de bonnes pratiques, mais formule également des interdictions visant, dans le contexte particulier de l'entreprise concernée, les comportements et usages qui sont constitutifs d'atteintes à la probité. À ce titre, il peut traiter notamment des cadeaux et invitations, des paiements de facilitations, des conflits d'intérêts, du mécénat, du sponsoring ainsi que, le cas échéant, de la représentation d'intérêts (lobbying) et des frais de représentation.

96. Il est par ailleurs possible d'intégrer le code de conduite dans un dispositif « d'éthique » (du type charte éthique) au périmètre plus large que la stricte lutte anticorruption, à la condition d'en permettre la parfaite lisibilité dans sa présentation.

- **L'articulation du code de conduite avec le règlement intérieur**

97. Dans les entreprises dans lesquelles il existe un règlement intérieur, le code de conduite y est intégré.

98. Lorsque l'entreprise n'est pas soumise à l'obligation de disposer d'un règlement intérieur, en France ou à l'étranger, le code de conduite est remis aux membres du personnel ou leur est rendu accessible, selon les modalités déterminées et tracées par l'entreprise.

- **Contenu**

99. Le code de conduite a vocation à être rédigé ou mis à jour postérieurement à l'élaboration de la cartographie des risques de corruption de l'entreprise, dans la mesure où il décrit les comportements à proscrire à partir des risques spécifiques à l'entreprise.

100. Le code de conduite contient des dispositions sur les types de comportements à proscrire auxquels les collaborateurs sont susceptibles d'être confrontés du fait de l'activité de l'entreprise. Une structuration en rubriques correspondant aux différents types de comportements à proscrire est encouragée.

101. Il est appuyé d'illustrations pertinentes au regard de l'entreprise et des risques définis dans sa cartographie des risques de corruption.

102. Il présente le dispositif d'alerte interne destiné à recueillir les signalements relatifs à l'existence de conduites ou de situations contraires au code de conduite.

103. Le code de conduite prévoit que les comportements proscrits et, plus généralement, les comportements non conformes aux engagements et principes de l'entreprise en matière de prévention et de détection des faits de corruption et de trafic d'influence sont susceptibles de faire l'objet de sanctions disciplinaires.

104. Le code de conduite mentionne le nom et les coordonnées des personnes qualifiées pour répondre aux questions des personnels (responsable de la fonction conformité, référent conformité ou intégrité…).

- **Formalisation et Accessibilité**

105. Le code de conduite, dont la préface est signée de l'instance dirigeante, matérialisant ainsi ses valeurs et son engagement en matière de prévention et de détection de la corruption, est rédigé en des termes qui le rendent intelligible et accessible à des non-spécialistes. Il est clair, sans réserve et sans équivoque. Il peut être traduit en une ou plusieurs langues étrangères afin de faciliter sa compréhension par les personnels ressortissants des États étrangers.

106. Le code de conduite est communiqué en interne et constitue un des éléments auxquels sont formés les collaborateurs de l'entreprise.

107. Le code de conduite sert également d'outil de communication externe dans les relations avec les clients, les fournisseurs, les intermédiaires et, plus généralement, les partenaires de l'entreprise concernée.

- **Mise à jour**

108. Le code de conduite est mis à jour régulièrement et notamment après la mise à jour de la cartographie des risques de corruption, par exemple à la suite d'une amélioration du dispositif anticorruption, d'une réorganisation ou d'une restructuration d'entreprise. Il comporte à cette fin une indication de sa date d'effet.

2. Formation et sensibilisation

109. Conformément au du 6° du II de l'article 17 de la loi, les personnes mentionnées au I sont tenues de mettre en œuvre « *un dispositif de formation destiné aux cadres et aux personnels les plus exposés aux risques de corruption et de trafic d'influence.* ».

- **Définition et objectifs**

110. Vecteur de la culture d'intégrité au sein de l'entreprise, un dispositif de sensibilisation et de formation efficace et adapté favorise une large diffusion des engagements pris par l'instance dirigeante en matière de lutte contre la corruption, leur appropriation par les collaborateurs et la constitution d'un socle de connaissances commun aux différents personnels de l'entreprise.

111. Une action de sensibilisation permet aux participants d'être mieux informés et réceptifs sur les sujets qui leur sont présentés.

112. Une action de formation consiste à procurer les connaissances et les compétences nécessaires à l'exercice d'une activité ou d'un métier. Elle s'intègre dans le plan de formation général de l'entreprise.

113. Le dispositif de sensibilisation et de formation anticorruption doit :

  - être coordonné avec les autres mesures et procédure du dispositif anticorruption. Ex : formation au contenu du code de conduite, formation prioritaire des personnes évaluées à risque par la cartographie, formation et sensibilisation à l'utilisation des dispositifs d'alerte…
  - tenir compte des risques spécifiques auxquels sont exposées les différentes catégories de personnels.

- **Le dispositif de sensibilisation destiné à tous les collaborateurs**

114. Si le dispositif de formation aux risques s'adresse prioritairement aux cadres et personnels les plus exposés, il est recommandé d'organiser une sensibilisation de l'ensemble des personnels.

115. Les actions de sensibilisation, destinées à tous les collaborateurs, portent notamment sur :

- l'engagement de l'instance dirigeante et le code de conduite ;
- les atteintes à la probité en général, leurs enjeux, leurs formes et les sanctions encourues, qu'elles soient disciplinaires ou pénales ;
- le comportement à adopter face à des faits de corruption, le rôle et les responsabilités de chacun ;
- le dispositif d'alerte interne.

116. Quelles que soient les modalités retenues, ces actions de sensibilisation visent à favoriser la prise de conscience des enjeux du phénomène de corruption dans l'entreprise et son environnement.

- **Formation obligatoire destinée aux cadres et aux personnels les plus exposés**

117. La formation des cadres et personnels les plus exposés permet de les alerter à la fois sur la nécessaire vigilance dont ils devront faire preuve dans l'exercice de leurs activités, mais également sur les comportements qu'ils devront adopter face aux situations à risques.

118. Ces formations visent à ce que les cadres et les personnels les plus exposés s'approprient le dispositif anticorruption de l'entreprise.

119. À terme, la formation a pour effet de limiter les risques identifiés dans la cartographie des risques de corruption.

120. Sur le fondement de la cartographie des risques, le responsable des ressources humaines identifie, avec l'aide du responsable de la fonction conformité (ou tout autre responsable désigné), les cadres et les personnels les plus exposés aux risques de corruption, c'est-à-dire les personnes en charge ou participant aux processus à risque.

121. Il peut s'agir, en particulier :

- des cadres et des personnels en relation avec des tiers exposés (commerciaux, acheteurs, etc.) ;
- des personnels qui participent à la mise en œuvre du dispositif anticorruption.

122. D'autres éléments, comme les fiches de poste, peuvent servir de base à l'identification des cadres et personnels exposés.

123. Le contenu des formations varie selon qu'elles s'adressent aux cadres et aux personnels les plus exposés aux risques de corruption ou à d'autres catégories de personnes.

124. Ce contenu est adapté à la nature des risques, aux fonctions exercées et aux zones géographiques d'activité de l'entreprise. Il est actualisé régulièrement, en lien avec la mise à jour de la cartographie des risques.

125. La formation implique une compréhension et une connaissance :

- des processus et des risques induits ;
- des infractions d'atteintes à la probité ;
- des diligences à accomplir et des mesures à appliquer pour réduire ces risques ;
- des comportements à adopter face à une sollicitation indue ;
- des sanctions disciplinaires encourues en cas de pratiques non conformes.

126. Le tronc commun de ces formations porte sur :

- l'engagement de l'instance dirigeante et le code de conduite anticorruption ;

- la corruption en général, ses enjeux et ses formes ;
- les obligations juridiques applicables et les sanctions afférentes ;
- le dispositif de conformité anticorruption ;
- le comportement à adopter, le rôle et les responsabilités de chacun face à des faits de corruption ;
- le dispositif d'alerte anticorruption.

127. En complément, des thématiques spécifiques sont traitées, selon les fonctions exercées par les participants et les risques spécifiques auxquels ils sont confrontés. Les outils de détection des atteintes à la probité peuvent être une thématique couverte par la formation à destination des personnels chargés d'une fonction de contrôle.

128. Les personnels et cadres les plus exposés sont formés rapidement après leur prise de fonction. Les formations sont régulièrement dispensées tout au long de l'exercice de leur fonction.

129. Les formations sont mises en œuvre avec des outils adaptés. Elles doivent être accessibles et dispensées dans une langue comprise par les publics auxquels elles s'adressent.

130. Les formations sont pragmatiques et pédagogiques. À l'instar du code de conduite, elles s'appuient notamment sur des cas pratiques et des scénarios personnalisés par public et adaptés aux risques de corruption identifiés dans la cartographie des risques.

131. Des membres de l'entreprise peuvent être invités à faire partager leur expérience en la matière, leurs réactions et les conclusions qu'ils en ont tirées, donnant ainsi lieu à des échanges au plus près des contraintes opérationnelles. Les mises en situation peuvent être utiles pour favoriser une appropriation des règles dans l'exercice quotidien des fonctions.

132. La mise en place d'outils permettant de vérifier la bonne compréhension des formations comme, par exemple, un contrôle de connaissances est à encourager. Ce contrôle de connaissance peut être effectué au cours de la formation et passé un certain délai, afin de s'assurer que les connaissances ont bien été assimilées.

133. Les formations peuvent être assurées par l'entreprise ou être mises en œuvre par un organisme extérieur, sous le contrôle de l'entreprise.

- **Contrôle et suivi du dispositif de formation**

134. La mise en place d'indicateurs permet d'assurer le suivi du dispositif de formation y compris dans l'hypothèse d'une externalisation des formations. Ces indicateurs peuvent inclure les items suivants :

- taux de couverture de la formation au regard du public visé ;
- nombre d'heures de formation sur la conformité et le dispositif anticorruption.

135. La qualité des formations et leur suivi, ainsi que l'identification des participants font l'objet d'un contrôle.

136. Dans l'hypothèse d'une externalisation des formations, le responsable de la fonction conformité (ou tout autre responsable désigné) doit non seulement être informé du calendrier des formations et de leur contenu pédagogique, mais aussi contrôler le déploiement du dispositif et les indicateurs associés.

3. L'évaluation de l'intégrité des tiers

137. Le 4° du II de l'article 17 de la loi prévoit que les personnes mentionnées au I mettent en œuvre « *des procédures d'évaluation de la situation des clients, fournisseurs, de premier rang et intermédiaires au regard de la cartographie des risques.* »

- **Définition et objectifs de l'évaluation de l'intégrité des tiers**

138. Les évaluations sont réalisées à partir de la cartographie des risques de corruption. Elles concernent notamment les clients, les fournisseurs de premier rang et les intermédiaires.

139. Elles visent :

  - d'une part, à permettre de décider d'entrer en relation avec un tiers, de poursuivre une relation en cours ou d'y mettre fin ;
  - d'autre part, d'optimiser l'efficacité des mesures de prévention et de détection de la corruption et de trafic d'influence.

- **Articulation du dispositif d'évaluation avec d'autres dispositifs (dont la lutte contre le blanchiment de capitaux et la lutte contre le financement du terrorisme LCB-FT)**

140. Les évaluations des tiers qui doivent être mises en œuvre doivent être distinguées des obligations de vigilance à l'égard de la clientèle auxquelles sont assujetties les personnes définies à l'article L. 561-2 du code monétaire et financier dans le cadre de la lutte contre le blanchiment des capitaux et le financement du terrorisme (article L.561-1 et suivants du code monétaire et financier).

141. Elles peuvent néanmoins être mises en œuvre à travers un dispositif unique, pour autant que ce dernier permette de détourer le risque spécifique de corruption et de trafic d'influence.

- **Champ d'application de l'évaluation : les tiers concernés**

142. La notion de « tiers » correspond aux clients, fournisseurs de premier rang et intermédiaires, quel que soit leur statut juridique (personne physique ou morale, de droit privé ou public), entretenant avec l'entreprise des relations qui peuvent les exposer à des risques potentiels de corruption et de trafic d'influence. L'entreprise peut également décider d'évaluer d'autres catégories de tiers, comme ses cibles d'acquisitions, ses bénéficiaires d'action de sponsoring ou de mécénat.

143. L'entreprise s'assure, en particulier pour les prestataires ou intermédiaires, que le recours à ces tiers est justifié et que leur prestation répond à un besoin avéré. Elle identifie également les raisons qui conduisent à retenir un tiers plutôt qu'un concurrent. Par exemple, constitue une alerte pour une entreprise le fait que le tiers soit recommandé ou imposé par le client.

144. La mise en place d'une base de données interne dédiée aux tiers est de nature à faciliter la réalisation et la gestion de leur évaluation.

145. Cette dernière doit être actualisée et sécurisée. Cette démarche suppose notamment l'adoption de procédures formalisées et sécurisées de création, validation, modification et suppression des tiers enregistrés dans la base, avec un respect strict de la répartition des tâches et des habilitations.

146. L'entreprise peut recenser de manière exhaustive ses tiers par catégorie. Cette approche a pour objet de déterminer *ex ante*, sur le fondement de la cartographie des risques, les catégories de tiers qui lui semblent les plus sensibles aux risques de corruption et de trafic d'influence.

147. La nature et la profondeur des évaluations à réaliser et des informations à recueillir sont déterminées en fonction des différents groupes homogènes de tiers présentant des profils de risques comparables, tels que la cartographie des risques permet de les identifier. Ainsi, les catégories de tiers jugées pas ou peu risquées pourront faire l'objet d'une évaluation simplifiée tandis que les catégories les plus risquées nécessiteront une évaluation approfondie.

148. Au sein de chaque catégorie de tiers qui nécessite une évaluation, chacun des tiers est évalué individuellement, en fonction de ses particularités. Les procédures d'évaluation des tiers visent en effet à apprécier le risque spécifique induit par la relation entretenue ou qu'il est envisagé d'entretenir avec un tiers donné.

149. L'évaluation de l'intégrité des tiers permet à l'entreprise d'apprécier des situations individuelles, ce que ne permet pas la cartographie des risques (et éventuellement la cartographie des tiers). Un tiers, considéré comme appartenant à une catégorie peu risquée dans la cartographie des risques, peut être requalifié en tiers risqué à l'issue de son évaluation individuelle. De même, un incident, une alerte, une condamnation concernant un tiers dont la catégorie est jugée peu risquée ou dont le comportement évolue au cours de la relation, peut conduire l'entreprise à réaliser une évaluation plus poussée ou à l'évaluer en priorité.

- **Modalités d'évaluation de l'intégrité des tiers**

150. Trois niveaux d'acteurs participent aux évaluations :

- le personnel en charge des évaluations et qui en est responsable, collecte les informations et documents utiles à l'évaluation des tiers avec lesquels il est ou est appelé à être en relation. Il émet une première appréciation. Cette appréciation vaut décision dans les cas considérés comme peu risqués ;
- le service de la conformité (ou tout autre responsable désigné) apporte son expertise et ses conseils au personnel en charge des évaluations. Il accompagne le niveau opérationnel dans l'appréciation des cas les plus risqués et dans la prise de décision ;
- l'instance dirigeante décide des suites à donner aux cas les plus risqués que lui communiquent les services concernés.

151. L'entreprise peut, en tant que de besoin, avoir recours à des prestataires externes, notamment lorsqu'elle n'est pas en mesure d'obtenir par elle-même les informations ou documents, ou lorsque le tiers réside ou intervient dans un pays où elle n'est pas implantée. L'entreprise demeure responsable de la qualité et de la pertinence des évaluations réalisées dans ce cadre.

152. La procédure d'évaluation de l'intégrité des tiers est formalisée.

153. La nature des informations et documents utiles à l'évaluation des tiers est déterminée par l'entreprise sur le fondement de sa cartographie des risques.

154. À titre indicatif, les évaluations peuvent inclure :

- la collecte d'informations au moyen de la consultation de listes internes à l'entreprise ;
- la collecte d'informations en sources ouvertes, de documents publics ou à disposition du public (par exemple : articles de presse, états financiers, décisions de justice lorsqu'elles sont publiées…) ;
- la vérification de la présence du tiers ou de ses bénéficiaires effectifs, tels que définis par les articles R. 561-1 et R. 561-2 du code monétaire et financier, de ses dirigeants ou de ses administrateurs, sur les listes des personnes physiques et morales sanctionnées (notamment la liste des personnes exclues des marchés publics financés par la banque mondiale, les banques

de développement ainsi que la liste des personnes sous sanctions financières et internationales des ministères économiques et financiers) ;

- la collecte d'informations dans des bases de données commercialisées par des prestataires spécialisés ;
- la collecte d'informations et de documents auprès du tiers, au moyen par exemple d'un questionnaire, d'un entretien, d'un audit, d'un processus interne d'agrément ou de certification.

155. Les informations ci-après sont obtenues, dans le respect des réglementations applicables, notamment celles relatives à la protection des données personnelles. Elles portent notamment sur l'identité du tiers, l'actionnariat, le secteur d'activité, la capacité professionnelle et l'intégrité du tiers.

156. L'entreprise recense les principaux éléments d'identité du tiers : nom, raison ou dénomination sociale, forme juridique de la structure, date de création, effectifs, chiffre d'affaires, capital, secteur(s) d'activité, domaines de compétences (notamment pour les intermédiaires et prestataires de services), implantation géographique.

157. L'entreprise identifie les noms, prénoms des principaux actionnaires, ainsi que les bénéficiaires effectifs.

158. L'entreprise apprécie la sensibilité du secteur d'activité du tiers au regard du risque de corruption et de trafic d'influence. Elle peut s'appuyer pour cela sur sa cartographie des risques de corruption ainsi que sur l'expérience qu'elle tire de ses activités. En complément, elle peut s'appuyer sur des analyses externes d'entreprises internationales ou d'organisations non gouvernementales.

159. L'entreprise s'assure que le tiers (en particulier s'il s'agit d'un intermédiaire ou prestataire) dispose de l'expérience, des qualifications et des compétences nécessaires à la réalisation de sa mission. À ce titre, elle peut demander au tiers de lui communiquer les références professionnelles qu'elle jugera nécessaires en fonction des données déjà recueillies (date de constitution, date du lancement de l'activité, etc.). Le manque de qualification ou d'expérience peut être défini comme un facteur aggravant lors de l'évaluation du niveau de risque du tiers.

160. L'entreprise recherche si le tiers, ses dirigeants, ses principaux actionnaires et ses bénéficiaires effectifs font ou ont fait l'objet d'informations défavorables, d'allégations, de poursuites ou de condamnations pour atteintes à la probité (ou le recel et le blanchiment de ces infractions).

161. La collecte de données personnelles relatives à l'intégrité du tiers doit respecter les normes régissant la protection des données.

162. L'entreprise peut également s'assurer que le tiers a mis en œuvre un dispositif de conformité anticorruption. Le fait que le tiers ne communique pas sur la mise en place d'un tel dispositif et ne le documente pas peut être considéré comme un facteur de risque.

163. Les relations public/privé présentent un risque identifié en termes de corruption. Il est pertinent que l'entreprise identifie les interactions que le tiers peut avoir avec des agents publics, *a fortiori* lorsqu'il s'agit de personnes politiquement exposées, au sens de l'article L 561-10 du code monétaire et financier.

- **Appréciation du niveau de risque du tiers**

164. L'entreprise apprécie le niveau de risque du tiers à partir des informations et documents collectés d'une part, et de l'analyse des conditions dans lesquelles s'inscrit la relation envisagée (ou de l'analyse de la nature et de l'objet de la relation), d'autre part. Elle tient compte également de facteurs aggravants comme le risque pays ou le comportement du tiers.

165. Certaines relations comportent un risque aigu de corruption comme, par exemple, le cas d'un tiers ayant pour mission d'assister l'entreprise dans l'obtention de contrats : d'une part, l'entreprise peut inciter le tiers à se livrer à des pratiques non conformes de façon à contourner son dispositif anticorruption ; d'autre part, le tiers peut se livrer à de telles pratiques de sa propre initiative, sans que l'entreprise n'en soit informée.

166. L'établissement d'une relation financière de longue durée ou à forte valeur peut constituer un facteur de risque lors de l'évaluation du niveau de risque du tiers. Par ailleurs, l'utilisation de certaines devises est également un élément à prendre en considération du fait de l'extraterritorialité de certaines législations anticorruption étrangères. De la même manière, le niveau de dépendance économique de l'entreprise vis-à-vis du tiers ou du tiers vis-à-vis de l'entreprise peut constituer un risque.

167. L'entreprise vérifie que le montant de la rémunération est cohérent avec la nature et le volume des biens ou services vendus par le tiers, et conforme au prix du marché. Une incohérence peut constituer un signal d'alerte et nécessite d'en justifier les raisons.

168. Le versement de commissions liées à l'obtention de contrats constitue un facteur de risque lors de l'évaluation du niveau de risque du tiers.

169. La localisation du compte bancaire du tiers peut constituer un facteur de risque lors de l'évaluation du niveau de risque du tiers (par exemple, si le compte bancaire est domicilié dans un État figurant dans la liste des États et territoires non coopératifs).

170. De plus, certaines modalités de paiement, dont les paiements en espèces, les paiements transfrontaliers, les paiements effectués sur présentation de factures non détaillées peuvent constituer des facteurs de risque lors de l'évaluation du niveau de risque du tiers.

171. Si le tiers n'est pas implanté sur le territoire français ou si la prestation est réalisée à l'étranger, la sensibilité du pays au risque de corruption donne lieu à une analyse au regard de l'expérience de l'entreprise et, en complément, au moyen notamment :

- de la liste des pays sous sanctions financières et internationales publiée par les ministères économiques et financiers ;
- des rapports de suivi de l'OCDE concernant la mise en œuvre de la convention sur la corruption d'agents publics étrangers dans les transactions commerciales dans les pays signataires ;
- de l'indice de perception de la corruption dans le secteur public publié chaque année par l'organisation non-gouvernementale *Transparency International* ;
- de l'enregistrement du tiers dans un État non coopératif ou dans un pays à législation non équivalente qui peut être défini comme un facteur de risque lors de l'évaluation du niveau de risque du tiers.

172. Le comportement du tiers est pris en compte dans l'évaluation du risque : le fait par exemple que le tiers refuse de fournir ou tarde à fournir les informations ou documents demandés peut être considéré comme un facteur de risque lors de son évaluation.

173. L'entreprise peut évoluer dans un écosystème regroupant plusieurs intervenants, sans pour autant être liée avec chacun d'entre eux (exemple : chaînes contractuelles). Dans ce cas, il est recommandé de s'assurer que les tiers avec lesquels l'entreprise est liée effectuent l'évaluation de leurs propres tiers conformément aux paragraphes précédents.

- **Conclusions à tirer des évaluations**

174. La décision est prise par les acteurs appropriés en fonction notamment du stade de la relation d'affaires (entrée en relation ou renouvellement…), de la catégorie à laquelle appartient le tiers et de son niveau de risque.

175. À la suite de l'évaluation du niveau de risque, il est décidé :

- d'approuver la relation – avec ou sans mesures de vigilance renforcée ;
- de mettre un terme à la relation ou de ne pas l'engager ;
- de reporter la prise de décision (pour cause d'évaluations complémentaires, par exemple).

176. Les personnes à l'origine de la décision sont clairement identifiées dans l'entreprise.

177. L'absence de facteurs de risque en suite d'évaluation ne garantit pas que la relation avec le tiers soit absolument dénuée de risque. À l'inverse, l'identification de facteurs de risques n'interdit pas la relation, mais doit conduire l'entreprise à prendre les mesures de vigilance appropriées pendant la relation.

- **Mesures de vigilance prévention à déployer en cours de relation d'affaires**

178. Les mesures de prévention et de détection de la corruption devant être adaptées à l'environnement de chaque entreprise, il revient à cette dernière de définir les mesures qu'elle juge cohérentes avec son modèle économique.

179. Dans ce cadre, l'entreprise peut utilement envisager l'une ou plusieurs des options suivantes :

- informer le tiers de l'existence de son programme anticorruption en communiquant, par exemple, le code de conduite ;
- former ou sensibiliser le tiers au risque de corruption et de trafic d'influence ;
- exiger du tiers un engagement écrit de lutte anticorruption ou insérer une clause permettant à l'entreprise de mettre un terme à la relation contractuelle en cas de manquement à la probité si la nature juridique du contrat le permet ;
- exiger du tiers qu'il vérifie l'intégrité de ses sous-traitants afin de sécuriser la chaîne contractuelle.

- **Suivi de la relation contractuelle avec le tiers**

180. La relation contractuelle doit être clairement établie afin d'en contrôler la bonne exécution.

181. À cet égard, l'entreprise doit avoir une visibilité complète sur les paiements reçus de tiers ou effectués aux tiers afin de s'assurer que la rémunération et les modalités de paiement sont conformes aux dispositions contractuelles. Les services financiers et comptables alertent le responsable de la conformité ou tout autre responsable désigné lorsque des modalités anormales de paiement sont exigées (par exemple : des paiements en espèces ou un changement de domiciliation du compte bancaire vers un pays ou territoire non coopératif en matière judiciaire ou fiscale, ou faisant l'objet d'un embargo).

- **Renouvellement et mise à jour des évaluations des tiers**

182. Le processus d'évaluation est reconduit de manière périodique, en fonction de la catégorie et du niveau de risque du tiers. À ce titre, il est utile de fixer, lors de toute entrée en relation, une date de renouvellement.

183. Un changement significatif dans la situation du tiers comme, par exemple, un changement de bénéficiaire effectif, une fusion de deux entités ou l'acquisition d'une nouvelle entité donne lieu à une nouvelle évaluation de celui-ci.

184. Une simple mise à jour des informations sur le tiers est possible, lorsque l'entreprise recueille, en cours de relation, des informations qui n'ont pas d'impact sur son niveau de risque.

185. Le processus de renouvellement sera l'occasion de s'assurer que le tiers a respecté ses engagements anticorruption tout au long de la relation.

- **Suivi du processus d'évaluation des tiers**

186. Un suivi du dispositif d'évaluation des tiers est mis en place et comprend notamment :

  - des indicateurs portant sur les évaluations réalisées ;
  - des indicateurs de renouvellement traçant le respect des fréquences de révision des évaluations des tiers ;
  - des résultats des contrôles de premier et de deuxième niveau ;
  - des indicateurs de renouvellement prioritaire, suite à un plan ponctuel de régularisation issu des contrôles de deuxième et de troisième niveau, consistant à traiter les cas échus ou non conformes.

187. L'ensemble de ces indicateurs et résultats peuvent, en fonction de leur objet, être transmis à la hiérarchie et au responsable de la conformité ou tout autre responsable désigné.

- **Conservations des informations sur les tiers**

188. L'intégralité du dossier d'évaluation du tiers ainsi que l'historique des modifications sont à conserver pendant 5 ans après la cessation de la relation d'affaires (ou après la date d'une opération occasionnelle), sous réserve d'une législation plus exigeante.

II.4) Détection de la corruption

1. Dispositif d'alerte anticorruption

189. Conformément au 2° du II de l'article 17 de la loi, l'entreprise est tenue de mettre en œuvre « un dispositif d'alerte interne destiné à permettre le recueil des signalements émanant d'employés et relatifs à l'existence de conduites ou de situations contraires au code de conduite de la société ».

- **Définition et objectifs**

190. Le dispositif d'alerte interne anticorruption est la procédure mise en œuvre par les entreprises afin de permettre à leurs employés de porter à la connaissance d'un référent dédié, un comportement ou une situation potentiellement contraire au code de conduite, afin d'y mettre fin et de prendre les sanctions appropriées, le cas échéant.

- **Articulation des différents dispositifs d'alerte**

191. Différents dispositifs d'alerte professionnelle, prévus par des textes législatifs spécifiques, coexistent, notamment en application de :

  - l'article 8, III de la loi n° 2016-1691 du 9 décembre 2016 ;
  - l'article 17, II, 2° de la loi n° 2016-1691 du 9 décembre 2016 ;
  - l'article L.225-102-4 du code de commerce ;
  - les articles L.4133-1 et suivants du code du travail ;
  - l'article R.822-33 du code de commerce.

192. Le dispositif d'alerte interne anticorruption se distingue des procédures à mettre en œuvre en matière de protection des lanceurs d'alerte en application des articles 6 à 15 de la loi n° 2016-1691 du 9 décembre 2016.

193. Dans la mesure où les dispositifs de recueil des signalements prévus par les articles 6 à 15, et le dispositif d'alerte interne anticorruption peuvent concerner pour partie les mêmes faits et situations, il est possible de mettre en place un seul et unique dispositif technique de recueil de ces signalements dans le respect des recommandations qui suivent.

194. Le régime de protection des lanceurs d'alerte nécessite de veiller à garantir la protection de leurs droits et notamment la stricte confidentialité de leur identité, mais également des faits objets du signalement et des personnes visées par le signalement. La violation de la confidentialité doit être susceptible d'entraîner des sanctions disciplinaires.

195. La mise en place d'un dispositif technique unique de recueil des signalements nécessite également de différencier le traitement appliqué aux signalements relatifs à des soupçons ou des faits de corruption de celui appliqué aux autres signalements.

196. En outre, la mise en place d'un dispositif technique unique de recueil suppose d'ouvrir la possibilité de signalement non seulement aux personnels, mais aussi aux collaborateurs extérieurs et occasionnels[3].

[3] Collaborateur extérieur ou occasionnel (personnel intérimaire, stagiaire, prestataire de service, salarié des entreprises sous-traitantes, etc.)

197. Au-delà de la mise en place d'un dispositif de recueil des signalements, toute personne souhaitant signaler des faits relevant de l'article 6 de la loi du 9 décembre 2016 précitée peut les porter à la connaissance de son supérieur hiérarchique, direct ou indirect, ou d'un référent désigné par l'employeur.

198. Elle peut également l'adresser au Défenseur des droits afin d'être orientée vers l'organisme approprié pour le recueil de l'alerte.

199. Si ce signalement n'a pas fait l'objet de diligences de la personne destinataire dans un délai raisonnable, le lanceur d'alerte pourra, dans un deuxième temps, s'adresser à l'autorité judiciaire, à l'autorité administrative ou aux ordres professionnels.

200. Toutefois, si le signalement porte sur des atteintes au devoir de probité, il pourra être adressé directement à l'AFA.

201. Enfin, à défaut de traitement du signalement dans un délai de trois mois par l'un des organismes saisis, celui-ci pourra être rendu public.

202. En cas de danger grave et imminent ou en présence d'un risque de dommages irréversibles, le signalement relatif à des faits mentionnés à l'article 6 de la loi peut être adressé directement à l'autorité judiciaire, à l'autorité administrative ou aux ordres professionnels. Il peut également être rendu public.

- **Définition et protection du lanceur d'alerte**

203. Aux termes de l'article 6 de la loi du 9 décembre 2016 :

« *Un lanceur d'alerte est une personne physique qui révèle ou signale, de manière désintéressée et de bonne foi, un crime ou un délit, une violation grave et manifeste d'un engagement international régulièrement ratifié ou approuvé par la France, d'un acte unilatéral d'une entreprise internationale pris sur le fondement d'un tel engagement, de la loi ou du règlement, ou une menace ou un préjudice graves pour l'intérêt général, dont elle a eu personnellement connaissance. Les faits, informations ou documents, quel que soit leur forme ou leur support, couverts par le secret de la défense nationale, le secret médical ou le secret des relations entre un avocat et son client sont exclus du régime de l'alerte défini par le présent chapitre.* »

204. Cinq conditions cumulatives caractérisent un lanceur d'alerte :

- il s'agit d'une <u>personne physique</u> : une personne morale (exemple : association, syndicat professionnel…) ne peut donc pas être considérée comme lanceur d'alerte ;
- le lanceur d'alerte a <u>personnellement connaissance</u> des faits qu'il signale : il ne s'agit donc pas de rapporter des faits constatés par autrui, mais de rapporter des faits qu'il a personnellement constatés ;
- le lanceur d'alerte agit de manière <u>désintéressée</u> : il ne bénéficie d'aucun avantage et n'est pas rémunéré en contrepartie de sa démarche. Le soutien que le lanceur d'alerte est, le cas échéant, susceptible de rechercher s'il se sentait menacé (exemple : accompagnement par un syndicat de représentants du personnel) ne remet pas en cause l'absence d'intéressement à la démarche ;
- le lanceur d'alerte agit de <u>bonne foi</u> : le lanceur d'alerte doit agir en pensant réellement que son signalement est conforme à la règle de droit et n'est pas animé de la volonté de nuire à autrui.

Sur ce point, l'auteur d'allégations qu'il sait fausses ne peut être considéré comme « *de bonne foi* » et encourt les poursuites prévues par la loi à l'encontre des auteurs de dénonciations calomnieuses (article 222-10 du code pénal).

- les faits révélés sont graves : ce critère s'apprécie au regard de la loi, qui mentionne un crime ou un délit, une violation grave et manifeste d'un engagement international pris par la France, ou d'un acte d'une organisation internationale pris sur ce fondement, ou une menace ou un préjudice graves pour l'intérêt général. Les délits de corruption répondent à ce critère de gravité.

205. Si l'émetteur d'une alerte interne réunit les conditions requises pour être qualifié de lanceur d'alerte, il bénéficie alors de la protection suivante :

- le lanceur d'alerte est pénalement irresponsable dès lors que les critères de définition fixés par la loi sont remplis, que la divulgation de l'information « *est nécessaire et proportionnée à la sauvegarde des intérêts en cause* » et qu'elle intervient dans le respect des procédures de signalement des alertes (article 122-9 du code pénal) ;
- qu'il soit salarié ou agent public, civil ou militaire, le lanceur d'alerte ne peut être licencié, sanctionné ou discriminé d'aucune manière pour avoir signalé des faits dans le respect de la procédure de signalement des alertes (article L 1132-3-3 du code du travail ; article 6 ter A alinéa 2 de la loi n° 83-634 du 13 juillet 1983 ; article L. 4122-4 alinéa 2 du code de la défense).

- **Organisation du dispositif d'alerte**

206. Le dispositif d'alerte interne doit être adapté au profil de risque de l'entreprise.

207. La gestion de ce dispositif (y compris la fonction de référent) peut être réalisée au sein de l'entreprise ou sous-traitée à un tiers.

208. Le dispositif d'alerte interne anticorruption précise le rôle du supérieur hiérarchique, qui doit pouvoir orienter et conseiller ses collaborateurs, sauf dans l'hypothèse où il est lui-même l'auteur du comportement incriminé.

209. L'entreprise veille à la formation des personnes en charge du traitement de l'alerte, au respect de la confidentialité de son traitement et à l'absence de tout conflit d'intérêts ; elle veille également à la formation des supérieurs hiérarchiques.

210. Le dispositif d'alerte interne est présenté sans délai aux collaborateurs venant de rejoindre l'entreprise.

211. La gestion de ce dispositif (y compris la fonction de référent défini ci-dessous) peut être sous-traitée à un tiers, sous réserve que ce tiers dispose des compétences nécessaires au bon traitement des alertes et au respect des moyens permettant d'en garantir la confidentialité. Les prestations fournies dans ce cadre devront faire l'objet de contrôles réguliers. L'entreprise veillera à donner au tiers retenu les moyens de traiter les alertes, notamment en veillant à lui faciliter l'accès aux services internes concernés de l'entreprise.

- **Traitement des alertes**

212. La procédure d'alerte interne doit préciser les différentes étapes à suivre pour effectuer un signalement, les modalités de traitement par celui qui en est destinataire, le droit des personnes concernées (et notamment leur protection), et les mesures de sécurité et de conservation des données à caractère personnel.

213. Le dispositif d'alerte interne indique :

- le référent fonctionnellement désigné pour recueillir les alertes au sein de l'entreprise et, s'il est différent, le référent en charge de leur traitement ;
- les dispositions prises pour garantir la confidentialité de l'identité de l'auteur du signalement, des faits objets du signalement et des personnes visées par le signalement, y compris lorsque des vérifications ou lorsque le traitement du signalement nécessitent la communication avec des tiers. La violation de la confidentialité doit être susceptible d'entraîner des sanctions disciplinaires.

214. Le dispositif d'alerte est sécurisé et, le cas échéant, ses droits d'accès sont limités aux seuls personnels autorisés à recueillir les alertes ou à les traiter.

215. Dans l'hypothèse d'une mise en cause d'une ou plusieurs personnes, l'entreprise doit être vigilante quant à la réunion de preuves ou documents, notamment lorsque les personnes mises en cause dans l'alerte peuvent détruire des données ou documents les incriminant.

216. Le dispositif d'alerte interne précise les modalités d'accès au dispositif et d'échange d'informations avec l'auteur de l'alerte, notamment :

- les canaux pour effectuer une alerte : il peut s'agir d'une adresse électronique dédiée, d'un logiciel de gestion voire, pour certaines entreprises, d'une plateforme éthique spécifique. L'alerte peut aussi emprunter la voie hiérarchique. En tout état de cause, ces canaux doivent être aisément accessibles aux utilisateurs ;
- les conditions de transmission, par l'auteur du signalement, des informations ou documents produits à l'appui de son signalement ;
- en cas d'enquête interne, les informations et documents professionnels susceptibles d'être exploités dans ce cadre ;
- les dispositions prises pour informer sans délai l'auteur du signalement de la réception de son alerte et du délai nécessaire à l'examen de sa recevabilité. Il est à ce titre recommandé de mentionner que l'accusé de réception ne vaut pas recevabilité du signalement ;
- les dispositions prises pour informer de la clôture de la procédure l'auteur du signalement et, le cas échéant, les personnes visées par celui-ci.

217. Si un traitement automatisé des alertes est mis en place, la procédure doit indiquer les dispositions prises pour en assurer la conformité aux dispositions de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et à celles relatives à la protection des données personnelles. Une donnée à caractère personnel désigne toute information se rapportant à une personne physique identifiée ou identifiable.

218. Face à une multiplication croissante des obligations en matière de recueil des alertes, la CNIL a publié une délibération n° 2019-139 du 18 juillet 2019 portant adoption d'un référentiel relatif aux traitements de données à caractère personnel destinés à la mise en œuvre d'un dispositif d'alertes professionnelles.

219. Les alertes peuvent être adressées de manière anonyme. Le dispositif doit permettre une poursuite des échanges avec le lanceur d'alerte tout en lui conservant le bénéfice de l'anonymat (il est par exemple envisageable de demander à l'auteur de l'alerte de fournir une adresse électronique qui ne permette pas son identification ou l'adresse d'une boîte postale)

220. Il est essentiel de définir et formaliser la procédure d'enquête interne préalablement à son lancement, tout en étant vigilant tant sur le choix des acteurs de l'enquête que sur son déroulé. La procédure d'enquête doit par ailleurs prévoir *a minima* :

- les critères nécessaires au déclenchement d'une enquête ;
- les modalités de réalisation de l'enquête.

221. Les personnes chargées de mener l'enquête doivent être soumises à de très strictes obligations de confidentialité, qui doivent être formalisées.

222. En cas d'externalisation de l'enquête interne, la conformité des services fournis dans ce cadre par le prestataire sélectionné doit faire l'objet de contrôles réguliers au regard notamment du respect des règles de confidentialité et de protection des données.

223. La décision de diligenter une enquête interne relève de personnes qualifiées, désignées par l'instance dirigeante de l'entreprise.

224. L'instance dirigeante est au minimum informée des enquêtes ouvertes. Elle intervient dans les situations les plus sensibles.

225. À la suite d'une enquête interne, la rédaction formelle d'un rapport d'enquête est destinée à consigner l'ensemble des faits et preuves recueillies, à charge et à décharge, de nature à établir ou à lever le soupçon, ainsi que la méthode suivie. Le rapport d'enquête interne conclut sur la suite à donner au signalement.

226. Lorsque les soupçons apparaissent suffisamment étayés, ce rapport est communiqué à l'instance dirigeante afin qu'elle décide des suites à donner.

227. La démonstration, par l'enquête interne, d'un comportement contraire au code de conduite anticorruption doit donner lieu à l'application des sanctions disciplinaires prévues en tel cas, décidées par l'instance dirigeante.

228. Enfin, une action judiciaire pourra être diligentée à l'encontre de la personne physique concernée si l'entreprise décide de porter les faits à la connaissance de l'autorité judiciaire par le moyen d'une plainte ou d'un simple signalement. Elle est même tenue de le faire si elle relève des autorités énumérées à l'article 40 du code de procédure pénale.

229. Les faits portés à la connaissance des instances dirigeantes par ces signalements doivent permettre d'actualiser la cartographie des risques, en respectant la confidentialité garantie par le dispositif, et d'en tirer les conséquences sur les améliorations à apporter aux éléments du dispositif de prévention et de détection de la corruption (plan de formation, code de conduite, évaluation de l'intégrité des tiers).

- **Périmètre**

230. Le dispositif d'alerte est à déployer sur l'ensemble du périmètre des entités contrôlées par l'entreprise. Il est à adapter aux spécificités de chaque entité (activité, taille, législation locale…).

- **Mise en œuvre du dispositif d'alerte interne**

231. Les étapes suivantes sont à réaliser :

- Établissement d'une procédure formalisée qui prévoit notamment ~~l~~a mise en place d'un comité intégrant des personnes qualifiées. Ce comité assure une prise de décision collégiale sur les suites à réserver aux alertes reçues.

- Insertion d'un chapitre sur le dispositif d'alerte dans le code de conduite renvoyant à ladite procédure ;
- Diffusion de la procédure d'alerte interne à l'ensemble des personnels par tous moyens (courrier de la direction, affichage, site intranet, remise en main propre…) permettant de s'assurer que chaque personne concernée en a connaissance et y a accès. Dans le cas d'un dispositif d'alerte commun à l'alerte anticorruption et à d'autres dispositifs légaux, la procédure doit être également diffusée aux collaborateurs occasionnels. L'entreprise peut décider d'ouvrir son dispositif d'alerte aux tiers. L'entreprise peut choisir de mettre à profit ses outils de communication externes pour mentionner l'existence de son dispositif d'alerte (par exemple son site internet, les documents remis à ses tiers…) ;
- Présentation du dispositif d'alerte dans le cadre des actions de sensibilisation de l'ensemble des personnels ;
- Formation des personnels amenés à recueillir, gérer et traiter les alertes, notamment sur les obligations de confidentialité, et formation des personnels les plus exposés ;
- Mise en place des contrôles de premier et second niveau sur la procédure d'alerte interne et intégration du dispositif d'alerte (comme tous les autres outils du dispositif de prévention de la corruption) dans le plan de contrôle de l'audit interne au titre du contrôle de troisième niveau. Pour éviter toute situation de conflit d'intérêts ou d'autocontrôle, les trois niveaux de contrôles rappelés ci-dessus peuvent être adaptés. Il importe, le cas échéant, que le personnel qui traite l'alerte soit différent de celui qui en contrôle le bon traitement et qu'un contrôle *a posteriori* soit effectué.

- **Indicateurs**

232. Des indicateurs sont mis en place afin d'apprécier la qualité et l'efficacité du dispositif d'alerte (nombre d'alertes reçues, classées sans suite ou traitées, délais de traitement, problématiques soulevées…). Ces indicateurs sont transmis à l'instance dirigeante.

- **Archivage des alertes et de leur traitement**

233. La durée de conservation et d'archivage des données personnelles relatives à une alerte va différer suivant que l'alerte est ou non suivie d'effets.

234. Si le responsable du traitement décide de donner suite[4] à une alerte, ou qu'une action disciplinaire ou contentieuse est engagée, l'ensemble des données à caractère personnel collectées à l'occasion de l'instruction peuvent être conservées jusqu'au terme de la procédure, jusqu'à acquisition de la prescription (six ans) ou épuisement des voies de recours.

235. Dans le cas où l'instruction de l'alerte ne débouche sur aucune suite, les données à caractère personnel doivent être détruites ou anonymisées dans les deux mois suivants la clôture de l'instruction.

236. Pour les alertes recueillies par le biais d'un dispositif technique unique de recueil, et ne concernant pas des faits susceptibles d'être qualifiés de corruption ou de trafic d'influence, les durées de conservation sont encadrées, par le décret n° 2017-564 du 19 avril 2017 relatif aux procédures de recueil des signalements émis par les lanceurs d'alerte au sein des personnes morales de droit public ou de droit privé ou des administrations de l'État.

[4] « *L'expression "suites" désigne toute décision prise par l'organisme pour tirer des conséquences de l'alerte. Il peut s'agit de l'adoption ou de la modification des règles internes (règlement interne, charte éthique, etc.) de l'organisme, d'une réorganisation des opérations ou des services de la société, du prononcé d'une sanction ou de la mise en œuvre d'une action en justice* » cf. Guide pratique de la CNIL sur les durées de conservation).

2. Le contrôle interne des risques de corruption et de trafic d'influence

- **La contribution du dispositif de contrôle et d'audit interne à la prévention et à la détection des risques de corruption et de trafic d'influence**

237. L'article 17 de la loi impose aux entreprises qui y sont soumises de mettre en place des procédures de contrôles comptables et un dispositif de contrôle et d'évaluation interne des mesures et procédures composant le dispositif anticorruption.

238. Les entreprises sont généralement dotées d'un dispositif de contrôle et d'audit interne à vocation générale, qui peut comprendre jusqu'à trois niveaux :

- les contrôles de premier niveau visent à s'assurer, *a priori*, que les tâches inhérentes à un processus opérationnel ou support ont été effectuées conformément aux procédures édictées par l'entreprise. Ils peuvent être opérés par les équipes opérationnelles ou support ou par le responsable hiérarchique ;
- Les contrôles de deuxième niveau visent à s'assurer, *a posteriori*, selon une fréquence prédéfinie ou de façon aléatoire, de la bonne exécution des contrôles de premier niveau. Ils peuvent être réalisés par la fonction en charge du pilotage du dispositif, par une fonction qualité, la fonction de management du risque, le contrôle de gestion, la fonction conformité, etc.
- Les contrôles de troisième niveau, également appelés « audits internes », visent à s'assurer que le dispositif de contrôle est conforme aux exigences de l'entreprise, efficacement mis en œuvre et tenu à jour.

239. Au-delà de la mise en œuvre des obligations prévues par l'article 17 de la loi, ce dispositif de contrôle et d'audit interne à vocation générale peut permettre de couvrir plus largement les risques identifiés à travers la cartographie des risques de corruption.

240. En effet, l'entreprise est en mesure, sur le fondement de celle-ci :

- d'identifier des situations à risque, pas ou peu couvertes par des mesures de contrôle,
- d'identifier et d'évaluer les dispositifs de contrôle de premier, deuxième et troisième niveau en place de nature à maîtriser ces risques.

241. L'entreprise est ainsi invitée à s'assurer que son dispositif de contrôle et d'audit interne à vocation générale :

- couvre les situations à risques identifiées par sa cartographie des risques de corruption,
- est adapté à ces risques et en mesure de les maîtriser ;
- est régulièrement mis à jour en fonction des situations de risque rencontrées et du résultat des contrôles réalisés.

242. Les contrôles ainsi définis viennent compléter le plan d'actions afférent à la cartographie des risques de corruption.

243. Les contrôles ainsi définis sont formalisés au sein d'une procédure qui précise notamment les processus et situations à risques identifiés, la fréquence des contrôles et leurs modalités, les responsables de ces contrôles et les modalités de transmission de leurs résultats à l'instance dirigeante.

- **Les contrôles comptables**

244. Parmi les procédures de contrôle et d'audit interne, les procédures de contrôle et d'audit comptable, qui participent à la maîtrise des risques des entreprises, constituent un instrument privilégié de prévention et de détection de la corruption et du trafic d'influence.

245. La comptabilité d'une entreprise est un outil d'évaluation contenant et présentant des informations sur son activité ainsi que sur les éléments de son patrimoine incorporel, matériel et financier. Les écritures comptables sont saisies, classées, retraitées et agrégées en vue de produire des documents retraçant fidèlement le détail des opérations.

- Définition et objectifs

246. Les contrôles comptables prévus par l'article 17 de la loi (ci-après « contrôles comptables anticorruption ») ont pour objectif de « *s'assurer que les livres, registres et comptes ne sont pas utilisés pour masquer des faits de corruption ou de trafic d'influence* ».

- Articulation avec les contrôles comptables en place

247. Les entreprises possèdent des procédures de contrôles comptables générales qui permettent d'avoir l'assurance raisonnable de la qualité de l'information comptable. Elles garantissent la régularité, la sincérité et la fidélité des opérations comptables et financières.

248. Les contrôles comptables anticorruption :

- garantissent *in fine* le respect des mêmes principes que les contrôles comptables généraux (régularité, sincérité et fidélité des opérations comptables et financières) ;
- visent en particulier à détecter des opérations sans cause ou sans justification (paiements en tout ou partie non causés destinés à alimenter des « caisses noires ») ;
- reposent sur les mêmes méthodes que les contrôles comptables généraux et comportent par exemple des contrôles par sondages, par revue de cohérence, par confrontation avec la réalité physique (inventaire) ou par confirmation par un tiers.

249. Ils sont établis, parmi les contrôles généraux existants, par approfondissement ou en complément de ceux-ci, pour cibler les situations à risques mises en évidence dans la cartographie des risques de corruption de l'entreprise.

250. Peuvent, par exemple, représenter des situations à risque et ainsi être traités, s'ils ressortent de la cartographie des risques :

251. Les opérations telles que le sponsoring, le mécénat, les honoraires et les commissions, les frais de représentation et de déplacement, les frais de marketing et de communication, les cadeaux et invitations, les dons, les legs, etc. ;

- les flux atypiques (exemple : comptes d'attente ou transitoires) ;
- les opérations exceptionnelles ou à enjeu ;
- les opérations liées au recours à des tiers tels que des intermédiaires ou des consultants ;
- les flux financiers ou de matière vers des comptes ou des tiers présentant un niveau de risque élevé comme les intermédiaires ou les agents commerciaux ;
- Les engagements hors bilan comme :
  - Les engagements pour compte de tiers (par exemple dirigeants, filiales),
  - Les garanties,
  - Les cautions.

252. La gestion de certains comptes comptables peut également ressortir comme processus risqué lors de l'analyse des risques au cours de l'exercice de cartographie : c'est le cas notamment des comptes d'extourne, de rabais et remises, de dépenses diverses, de fonds de caisse. Des comptes bilanciels peuvent également comporter un niveau de risque élevé comme les écarts d'acquisition ou les comptes d'attente ou d'avance.

- Formalisation des contrôles comptables anticorruption

253. Les modalités des contrôles comptables anticorruption sont formalisées au sein d'une procédure rappelant notamment :

- l'objet et le périmètre des contrôles ;
- les rôles et responsabilités dans leur mise en œuvre ;
- les modalités d'échantillonnage des opérations à contrôler, le cas échéant ;
- la définition d'un plan de contrôle ;
- les modalités de gestion des incidents ;
- les critères de seuils ou de matérialité devant entraîner un contrôle.

- Contenu des contrôles comptables anticorruption

254. Les contrôles comptables anticorruption de premier niveau sont généralement effectués par les personnes en charge de la saisie et de la validation des écritures comptables. Ces personnes s'assurent que les écritures sont convenablement justifiées et documentées (en particulier les écritures manuelles).

255. Afin de limiter le risque lié à l'autocontrôle, il est recommandé de s'assurer que les écritures comptables à risque soient examinées et validées par un collaborateur indépendant de celui qui en a effectué la saisie.

256. Une validation croisée entre collaborateurs est satisfaisante pour des écritures inférieures à un seuil défini. Les écritures supérieures à ce seuil nécessitent une validation par la hiérarchie.

257. Les contrôles comptables anticorruption de deuxième niveau, réalisés par des personnes indépendantes de celles ayant réalisé les contrôles de premier niveau, sont réalisés tout au long de l'année.

258. Ils visent à s'assurer de la bonne exécution des contrôles comptables anticorruption de premier niveau. Ainsi, lors des contrôles par sondage, l'échantillon retenu doit être représentatif des risques inhérents aux opérations traitées (écritures manuelles, niveau d'habilitation et séparation des tâches notamment). Les modalités de l'échantillonnage sont définies en fonction d'une analyse préalable des différentes écritures et risques concernés pour en permettre la représentativité.

259. Dans l'hypothèse où des contrôles comptables anticorruption de premier niveau sont automatisés, les contrôles comptables anticorruption de deuxième niveau sont corrélativement renforcés.

260. Les résultats des contrôles comptables anticorruption de deuxième niveau donnent lieu à une synthèse conclusive incluant, en cas d'anomalies, la définition d'actions correctives dans le cadre d'un plan d'actions.

261. L'efficacité des procédures de contrôles comptables anticorruption est évaluée régulièrement dans le cadre de contrôles comptables de troisième niveau, également appelés « *audits comptables* ».

262. Ces audits comptables couvrent l'ensemble des dispositifs comptables afin de s'assurer que les contrôles comptables anticorruption sont conformes aux exigences de l'entreprise, efficacement mis en œuvre et tenus à jour.

263. Dans ce cadre, les contrôles comptables de troisième niveau apprécieront la pertinence et l'efficacité :

- de la gouvernance et des ressources allouées aux procédures de contrôles comptables anticorruption ;
- de la méthode d'élaboration (notamment de la prise en compte de la cartographie des risques de corruption) et de l'application des contrôles comptables anticorruption de premier niveau et de deuxième niveau.

Traitement des anomalies constatées

264. Le constat d'une anomalie peut amener à compléter certaines procédures comptables existantes pour y remédier.

265. Les cas d'anomalies alimentent également une mise à jour de la cartographie des risques de corruption et peuvent faire l'objet d'illustrations complémentaires dans le code de conduite et les supports de formation dédiés à la prévention de la corruption et du trafic d'influence en coordination avec le responsable de la fonction conformité.

266. Si l'anomalie relève d'un manquement dans la mise en œuvre des procédures ou du dispositif anticorruption, le responsable hiérarchique peut envisager des mesures envers l'auteur du manquement allant du simple rappel de la règle à la sanction, suivant l'importance du manquement constaté.

267. Si l'anomalie fait ressortir des soupçons ou des faits de corruption, elle doit être portée à la connaissance du responsable de la fonction conformité et de l'instance dirigeante qui peut décider de diligenter une enquête interne.

Externalisation

268. Les contrôles comptables anticorruption peuvent être mis en œuvre :

- en interne, par les services comptables et financiers ou par des services spécialisés (centres de services partagés, contrôle de gestion, audit interne…) que l'entreprise mobilise à cette fin ;
- en externe, par les entités que l'entreprise mandate à cette fin.

269. Au sein des entreprises qui ont l'obligation de nommer un commissaire aux comptes chargé de la certification des comptes, ce dernier participe, à l'occasion de ses vérifications et dans l'objectif qui lui est assigné, à la prévention des difficultés éventuelles de l'entreprise auditée, à la prévention et à la détection de la corruption et du trafic d'influence. Il est rappelé qu'il est tenu de révéler au procureur de la République les faits délictueux – y compris donc les faits de corruption et de trafic d'influence - dont il a connaissance au cours de sa mission.

3. Régime disciplinaire

- **Définition**

270. Le régime disciplinaire regroupe l'ensemble des mesures qu'une entreprise se réserve le droit de prendre à l'occasion d'un comportement qu'elle considère fautif.

271. Est notamment considéré comme une faute de nature à justifier l'application d'une sanction disciplinaire le non-respect des règles de discipline fixées par le règlement intérieur et donc par le code de conduite anticorruption qui y est intégré. Dans les entreprises d'au moins 20 salariés, le règlement intérieur est obligatoire. Une sanction ne peut alors être prononcée à l'encontre d'un salarié que si elle est prévue par le règlement intérieur.

- **Principe de gradation des sanctions**

272. La sanction disciplinaire doit être proportionnée à la faute commise. Elle relève de l'échelle des sanctions prévues par le régime disciplinaire.

- **Mécanisme**

273. L'engagement de l'instance dirigeante dans la maîtrise du risque de corruption implique, lorsque des manquements aux devoirs d'intégrité et de probité des personnels sont constatés, d'engager une procédure disciplinaire à leur encontre et de leur appliquer des sanctions proportionnées.

274. L'instance dirigeante n'est pas tenue d'attendre que soit rendue une décision pénale pour mettre en œuvre des sanctions disciplinaires si les faits sont avérés et que leur gravité le justifie. La mise en œuvre de ces sanctions peut en effet s'appuyer sur les constatations d'une enquête interne circonstanciée, permettant d'établir avec rigueur la matérialité des faits reprochés à la personne concernée.

- **Mise en place d'un registre des sanctions**

275. Le recensement des sanctions disciplinaires prononcées à l'encontre des personnels de l'entité favorise le renforcement des mécanismes de maîtrise des risques d'atteintes à la probité.

276. Quel que soit le support utilisé pour effectuer ce recensement, l'entreprise veillera à la stricte confidentialité de son contenu et l'établira dans le respect des règles de protection des données personnelles.

- **Communication interne**

277. La diffusion, sous un format garantissant la totale anonymisation, des sanctions disciplinaires peut être demandée par l'instance dirigeante, afin de rappeler la politique de tolérance zéro à l'égard de tout comportement contraire à l'intégrité et à la probité.

II.5) Contrôle et évaluation des mesures et procédures composant le dispositif anticorruption

1. Objectifs et modalités

278. Afin de s'assurer de l'adéquation et de l'efficacité des mesures et procédures visées au II de l'article 17 de la loi, l'entreprise développe un dispositif de contrôle et d'évaluation interne, qui peut être inséré dans son dispositif de contrôle et d'audit interne à vocation générale.

279. Ce dispositif répond à quatre objectifs :

- contrôler la mise en œuvre des mesures du dispositif anticorruption et tester leur efficacité ;
- identifier et comprendre les manquements dans la mise en œuvre des procédures ;
- définir des recommandations ou autres mesures correctives adaptées, si nécessaire, en vue d'améliorer l'efficacité du dispositif anticorruption ;
- détecter, le cas échéant, des faits de corruption ou de trafic d'influence.

280. Ces contrôles s'articulent autour des trois niveaux de contrôles susmentionnés.

281. Le responsable de la fonction conformité élabore, en concertation avec les responsables des contrôles de premier et de deuxième niveau, un plan de contrôle de deuxième niveau couvrant l'ensemble du dispositif anticorruption.

282. Pour chacun des contrôles, sont précisés l'objet et le périmètre, le ou les responsables en charge du contrôle, la méthode de contrôle (type de mesure, de pièces justificatives, d'analyse, et d'évaluation), le cas échéant, les modalités d'échantillonnage fondées sur une analyse des risques. De même, le plan prévoit la fréquence du contrôle, la formalisation attendue, la communication des résultats du contrôle et des mesures correctives pouvant être mises en place et les modalités de conservations des pièces afférentes aux contrôles.

283. Les manquements identifiés dans le cadre des contrôles de deuxième niveau font l'objet d'un rapport visé par le responsable de la fonction conformité dont une synthèse est communiquée à l'instance dirigeante et au service d'audit interne.

284. La pertinence et l'efficacité des mesures et procédures composant le dispositif anticorruption sont régulièrement évaluées par des contrôles de troisième niveau. Ces audits internes visent à s'assurer que le dispositif de prévention et de détection de la corruption est conforme aux exigences de l'entreprise, efficacement mis en œuvre et tenu à jour. L'audit interne est également invité à s'assurer que les situations de risque identifiées par la cartographie des risques de corruption sont couvertes par des mesures de prévention efficaces.

285. Les audits réalisés sont formalisés, documentés et conservés. Ils donnent lieu à la rédaction d'un rapport circonstancié et documenté relatant les éventuels manquements et détaillant les mesures correctives ainsi que les recommandations formulées. Ce rapport est communiqué à l'instance dirigeante.

2. Typologie de contrôles à déployer

286. Pour chaque mesure et procédure visée à l'article 17 de la loi, des contrôles de premier, deuxième et troisième niveaux sont définis et mis en œuvre.

287. L'AFA recommande que ces contrôles portent notamment sur les éléments suivants :

	288. **Cartographie des risques de corruption**
Contrôles de 1er niveau :	Les contrôles liés à la cartographie ne peuvent être réalisés qu'*a posteriori*, après son établissement et ses mises à jour. Aucun contrôle de premier niveau ne peut être réalisé dans ce cadre. Par ailleurs, le service en charge du pilotage du dispositif anticorruption, qui a participé à la mise en place de la cartographie ou à ses mises à jour ne peut réaliser de contrôle de second niveau, sauf à être en situation de contrôler le travail qu'il a lui-même produit.
Contrôles de 2e niveau :	
Contrôles de 3e niveau :	- Revue du périmètre de la cartographie, de la méthodologie mise en œuvre, du déploiement des plans d'actions y afférents ; - Analyse des insuffisances constatées et des incidents survenus (pour éventuelle mise à jour) ; - Analyse de la gouvernance et de la correcte allocation des ressources.
	Analyse du caractère systémique du dispositif
	- Analyse des illustrations retenues dans le code de conduite au regard des risques identifiés dans la cartographie ; - Analyse du ciblage et du contenu des formations au regard des risques identifiés dans la cartographie ; - Analyse des incidents révélés au travers du dispositif d'alerte ou des contrôles comptables et leurs conséquences sur la mise à jour de la cartographie ; - Analyse de l'adéquation du dispositif d'évaluation des tiers au regard des risques identifiés dans la cartographie.

	289. **Code de conduite**
Contrôles de 1er niveau :	- Validation *a priori* des opérations ou situations régies par les politiques ou procédures intégrées ou annexées au code de conduite (relatives notamment aux cadeaux et invitations).
Contrôles de 2e niveau :	- Contrôle régulier de la correcte réalisation des contrôles de premier niveau ; - Contrôle par échantillonnage du respect des politiques ou procédures intégrées ou annexées au code de conduite. *Par exemple : définition trimestrielle d'un échantillon de XX notes de frais sur la base d'une analyse des risques. Puis analyse de la cohérence du justificatif vis-à-vis de la déclaration, les noms des invités, le respect des seuils/des validations...* - Revue du contenu du code au regard de la loi et de la cartographie et de l'intégration, pour les entités concernées, du code de conduite au sein de leur règlement intérieur ; - Vérification, à chaque mise à jour de la cartographie, que les illustrations du code de conduite sont adaptées ;
Contrôles de 3e niveau :	- Contrôle de la correcte réalisation et de l'efficacité des contrôles de premier et deuxième niveau ; - Analyse de la communication, de la diffusion et de l'accessibilité du code de conduite et des politiques/procédures intégrées ou annexées.
	Analyse du caractère systémique du dispositif

	Par exemple, une analyse critique du contenu (notamment les illustrations) du code de conduite au regard des scénarios identifiés dans la cartographie et de l'intégration du contenu du code de conduite dans la formation.

	290. **Formation**
Contrôles de 1er niveau :	- Vérification de la présence des collaborateurs concernés et des connaissances qu'ils ont acquises lors des formations.
Contrôles de 2e niveau :	- Contrôle régulier de la correcte réalisation des contrôles de premier niveau ; - Vérification de la cohérence entre les publics ciblés dans la formation, le contenu de la formation et les risques auxquels ils peuvent être exposés tels qu'identifiés dans la cartographie ; - Revue de la participation des collaborateurs concernés et des éventuelles sanctions en cas de non-suivi de la formation.
Contrôles de 3e niveau :	- Contrôle de la correcte réalisation et de l'efficacité des contrôles de premier et deuxième niveau ; - Analyse de la gouvernance et de la correcte allocation des ressources. *Par exemple, analyse des modalités (présentiel/en ligne...) et du contenu de la formation destinée aux cadres et personnels les plus exposés au regard des risques qui leur sont propres.*
	Analyse du caractère systémique du dispositif
	Par exemple, analyse du ciblage et du contenu de la formation destinée aux cadres et personnels les plus exposés au regard des risques identifiés dans la cartographie. *S'assurer que les références au code de conduite et au dispositif d'alerte sont claires.*

	291. **Évaluation des tiers**
Contrôles de 1er niveau :	- Contrôle *a priori* de l'application de la/les procédure(s) d'évaluation des tiers. *Par exemple, vérifier en amont de l'entrée en relation avec un nouveau fournisseur :* *- que l'ensemble des documents prévus par la procédure (ex. : liste des bénéficiaires effectifs, réponses à un éventuel questionnaire...) ont été collectés ;* *- que les recherches nécessaires ont été effectuées (sources ouvertes, bases de données...) ;* *- que l'évaluation est conforme aux éléments analysés ;* *- que la décision d'entrer ou de refus d'entrer en relation a été correctement formalisée.*
Contrôles de 2e niveau :	- Contrôle régulier de la correcte réalisation des contrôles de premier niveau, sur la base d'un échantillonnage représentatif de dossiers ; - Vérification de la mise en place des mesures de vigilance et de leur suivi effectif ; - Vérification de la mise à jour des dossiers (renouvellement périodique de l'évaluation ou à la suite d'un signalement) ; - Contrôle de la pertinence des mesures de vigilance déployées.

Contrôles de 3e niveau :	- Contrôle de la correcte réalisation et de l'efficacité des contrôles de premier et deuxième niveau.
	Analyse du caractère systémique du dispositif
	Par exemple, contrôle de l'adéquation du dispositif d'évaluation des tiers avec les risques identifiés dans la cartographie. *S'assurer de la mise à jour des dispositifs de contrôles comptables au regard des risques identifiés à l'occasion des évaluations de tiers.*

	292. **Alerte interne**
Contrôles de 1er niveau :	- Contrôle du déploiement et de la correcte application de la procédure d'alerte. *Par exemple, contrôle de l'accessibilité des canaux, et communication large sur le dispositif d'alerte, accusé de réception, analyse de recevabilité de l'alerte, identification des rôles et responsabilités au sein de l'équipe en charge de l'investigation, clôture de l'investigation, information de clôture, sanctions et plans d'actions, respect de la confidentialité et de l'anonymat, suivi des mesures de protection...*
Contrôles de 2e niveau :	- Contrôle régulier de la correcte réalisation des contrôles de premier niveau, sur la base d'un échantillonnage représentatif de dossiers.
Contrôles de 3e niveau :	- Contrôle de la correcte réalisation et de l'efficacité des contrôles de premier et deuxième niveau ; - Analyse qualitative et quantitative des signalements reçus sur la période (Quels canaux utilisés ? Des signalements sont-ils remontés par d'autres canaux non identifiés ? Quels sujets visés ? ...) - Contrôle de la pertinence des réponses apportées aux signalements reçus.
	Analyse du caractère systémique du dispositif
	Par exemple, prise en compte des signalements dans la mise à jour de la cartographie, du dispositif d'évaluation des tiers ou des contrôles comptables. *Contrôle de l'existence d'une formation/information des collaborateurs sur le dispositif d'alerte et d'une formation spécifique pour les personnes en charge de leur traitement.*

	293. **Contrôles comptables**
Contrôles de 1er niveau :	- contrôle automatisé de certaines opérations ; - contrôle des habilitations ; - règle « des quatre yeux » : revue par un collaborateur différent de celui en charge de passer l'opération ; - contrôle de la correcte application des contrôles comptables anticorruption *avant réalisation de l'opération*
Contrôles de 2e niveau	- Contrôle régulier de la correcte réalisation des contrôles comptables anticorruption après réalisation de l'opération sur la base d'un échantillonnage représentatif de dossiers

Contrôles de 3e niveau	- Contrôle de la correcte réalisation et de l'efficacité des contrôles comptables de premier et deuxième niveaux ; - Analyse de la réalisation des contrôles comptables et de la correcte allocation des ressources ; - Analyse de la pertinence des contrôles comptables au regard des risques identifiés par la cartographie.
	Analyse du caractère systémique du dispositif
	Par exemple, analyse critique des procédures de contrôles comptables en place au regard des mises à jour de la cartographie des risques de corruption

	294. **Régime disciplinaire**
Contrôles de 1er niveau :	Le contrôle de la conformité du régime disciplinaire ne peut être effectué qu'*a posteriori*, une fois les sanctions prononcées.
Contrôles de 2e niveau	- Contrôle, pour chaque incident, de la prise de sanction ; - Vérification de l'adéquation entre l'incident et la sanction.
Contrôles de 3e niveau	- Contrôle de la correcte réalisation et de l'efficacité des contrôles de deuxième niveau.
	Analyse du caractère systémique du dispositif.
	Par exemple, analyse des sanctions mises en œuvre et de la nécessité de renforcer la communication de l'instance dirigeante ou les formations sur telle ou telle mesure composant le dispositif anticorruption.

295. Si l'entreprise a déployé au sein de son dispositif anticorruption d'autres mesures et procédures en complément des celles visées par l'article 17 de la loi, l'AFA recommande que ces mesures et procédures fassent également l'objet de contrôles à travers le dispositif de contrôle et d'évaluation internes mis en place.

296. Les contrôles de premier niveau sont formalisés et documentés.

297. Les contrôles de deuxième niveau font l'objet d'un plan de contrôle formalisé décrivant notamment le périmètre des contrôles, les rôles et responsabilités, la fréquence, les modalités d'échantillonnage, la formalisation attendue, le suivi des anomalies et les plans d'actions associés.

298. Les contrôles de troisième niveau font l'objet d'un programme d'audit formalisé décrivant notamment le périmètre des contrôles, les modalités d'échantillonnage, la formalisation attendue, le suivi des anomalies et les plans d'actions associés.

3. Gestion des insuffisances constatées et suivi des recommandations

299. Les manquements liés à la mise en œuvre des procédures - et potentiellement signalés par les contrôles et audits - sont analysés afin d'en identifier l'origine et d'y remédier.

300. Ces manquements peuvent conduire l'instance dirigeante à décider la mise en œuvre de sanctions disciplinaires (adaptées et proportionnées) à l'encontre de leurs auteurs.