

Avis et communications

AVIS DIVERS

MINISTÈRE DE L'ÉCONOMIE, DES FINANCES ET DE LA RELANCE

Avis relatif aux recommandations de l'Agence française anticorruption 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'intérêts, de détournement de fonds publics et de favoritisme

NOR : ECOZ2035293V

Version du 4 décembre 2020

Table des matières

I. – Dispositions générales

I.1) *Objet*

I.2) *Champ d'application*

I.3) *Portée juridique*

I.4) *Principes fondamentaux*

1. Principe de proportionnalité et périmètre d'intervention

2. Trois piliers indissociables

Premier pilier : l'engagement de l'instance dirigeante

Deuxième pilier : la cartographie des risques d'atteintes à la probité

Troisième pilier : mesures et procédures de maîtrise des risques d'atteintes à la probité

II. – Déclinaison des dispositions générales aux entreprises assujetties à l'article 17 de la loi

II.1) *Premier pilier : l'engagement de l'instance dirigeante*

1. Définition de l'instance dirigeante

2. Responsabilité de l'instance dirigeante

3. Moyens dédiés

II.2) *Deuxième pilier : la cartographie des risques*

1. Objectifs de la cartographie des risques

2. Caractéristiques de la cartographie des risques

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

II.3) *Troisième pilier : la gestion des risques*

A. – Prévention des risques

1. Code de conduite

2. Sensibilisation et formation

3. Évaluation de l'intégrité des tiers

B. – Détection

1. Dispositif d'alerte interne

2. Le contrôle interne

C. – Contrôle et évaluation du dispositif anticorruption

1. Objectifs et modalités

2. Typologie de contrôles à déployer

D. – Remédiation

1. Gestion et suivi des insuffisances constatées

2. Régime disciplinaire

III. – Déclinaison des dispositions générales aux acteurs publics assujettis au 3^o de l'article 3 de la loi

III.1) *Premier pilier : l'engagement de l'instance dirigeante*

1. Définition de l'instance dirigeante
2. Responsabilité de l'instance dirigeante
3. Moyens dédiés
4. Une politique de communication interne et externe adaptée

III.2) *Deuxième pilier : la cartographie des risques d'atteintes à la probité*

1. Objectifs de la cartographie des risques d'atteintes à la probité
2. Caractéristiques de la cartographie des risques d'atteintes à la probité
3. Les différentes étapes de mise en place d'une cartographie des risques d'atteintes à la probité

III.3) *Troisième pilier : la gestion des risques d'atteintes à la probité*

A. – Prévention des risques

1. Règles en matière de déontologie/éthique et code de conduite
2. Formation et sensibilisation
3. L'évaluation de l'intégrité des tiers

B. – Détection

1. Dispositif d'alerte interne
2. Le contrôle interne des risques d'atteintes à la probité

C. – Contrôle et évaluation interne du dispositif anticorruption

1. Objectifs et modalités
2. Typologie de contrôles à déployer
3. Gestion des insuffisances constatées et suivi des recommandations

D. – Remédiation

1. Gestion et suivi des insuffisances constatées
2. Régime disciplinaire

Annexe n° 1 : Le lanceur d'alerte

Annexe n° 2 : Exemple de scénarios de risques pour les acteurs publics

I. – Dispositions générales

I.1) *Objet*

1. Aux termes du premier alinéa du 2^o 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, dite loi Sapin II, dénommée, sauf indication contraire, « la loi » dans la suite de ces recommandations, 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. L'ensemble de ces faits, délictuels, sont définis au titre III du livre IV du code pénal, à la section 3 du chapitre II (« manquements au devoir de probité »), ainsi qu'à la section 1 du chapitre V (« corruption des personnes n'exerçant pas une fonction publique ») du titre IV. Pour la simplification des présentes recommandations et sauf indication contraire, l'ensemble de ces infractions seront indistinctement qualifiées d'« atteinte à la probité ».

3. Les présentes recommandations interprètent les dispositions de la loi relatives aux dispositifs de prévention et de détection de ces faits. Elles visent à mettre à jour et à enrichir les recommandations déjà émises sur ce sujet en décembre 2017, en tirant les enseignements de trois années d'exercice des missions de l'AFA.

4. La loi, ses décrets d'application, les présentes recommandations et les guides publiés sur le site internet de l'AFA constituent le référentiel anticorruption français. Ce dernier participe de la mise en œuvre des engagements internationaux de la France en matière de lutte contre la corruption.

5. Les présentes recommandations, qui entrent en vigueur le lendemain de leur publication, annulent et remplacent celles parues au *Journal officiel* de la République française le 22 décembre 2017.

I.2) *Champ d'application*

6. Les recommandations définissent les modalités de mise en œuvre des dispositifs de prévention et de détection des atteintes à la probité (ci-après dénommés « dispositifs anticorruption ») que peuvent déployer, de manière proportionnée en fonction de leur profil de risque, toutes les personnes morales de droit privé ou de droit public, de droit français ou de droit étranger (ci-après dénommées « organisations »), qui déploient leurs activités en France comme à l'étranger, quels que soient leur taille, leur forme sociale ou leur statut juridique, leur secteur ou domaine d'activité, leur budget ou leur chiffre d'affaires ou l'importance de leurs effectifs.

7. Elles ont également pour objectif d'aider les organisations assujetties à l'obligation de déployer un dispositif anticorruption à se conformer à la loi.

I.3) Portée juridique

8. Les présentes recommandations ne créent pas d'obligation juridique pour ceux à qui elles s'adressent. Les organisations mentionnées au paragraphe 7 sont libres d'adopter d'autres méthodes, sous réserve que leur mise en œuvre permette de se conformer à la loi.

9. L'AFA se réfère aux recommandations dans le cadre de ses missions de conseil et de contrôle. Elle ne se référera aux présentes que pour les contrôles ouverts à compter du sixième mois suivant celui de leur entrée en vigueur.

10. Ces recommandations sont opposables à l'AFA dans le cadre de ses activités de contrôle, en ce sens que les organisations mentionnées au paragraphe 7 peuvent s'en prévaloir si elles ont décidé de s'y conformer.

11. Ainsi, une organisation mentionnée au paragraphe 7 qui indique lors d'un contrôle de l'AFA avoir suivi les présentes recommandations bénéficie d'une présomption simple de conformité. Celle-ci ne peut être renversée que par la démonstration par l'AFA d'une application non effective, incorrecte ou incomplète des recommandations.

12. Une organisation mentionnée au paragraphe 7 qui déciderait de ne pas mettre en œuvre tout ou partie des méthodes préconisées dans ces recommandations ne peut être *a priori* considérée comme ne respectant pas la loi. Cependant, dans le cas où l'AFA contesterait lors d'un contrôle tout ou partie des mesures prises par cette organisation, il reviendrait à cette dernière de démontrer que les choix qu'elle a faits lui permettent de satisfaire aux exigences posées par la loi.

I.4) Principes fondamentaux

13. Dans la suite de ces recommandations, un dispositif anticorruption désigne l'ensemble de mesures prises et procédures mises en place par une organisation pour connaître, prévenir, détecter et sanctionner tout ou partie des faits mentionnés au paragraphe 1.

1. Principe de proportionnalité et périmètre d'intervention

14. Ces recommandations sont adaptées par les organisations qui y ont recours en fonction de leur profil de risques, qui est affecté par différents paramètres, notamment les activités, compétences ou type de produit ou service qu'elles exercent ou fournissent, leur structure de gouvernance, leur organisation, leur taille, leur domaine ou secteur d'activité, leurs implantations géographiques, et les différentes catégories de tiers avec lesquels elles interagissent.

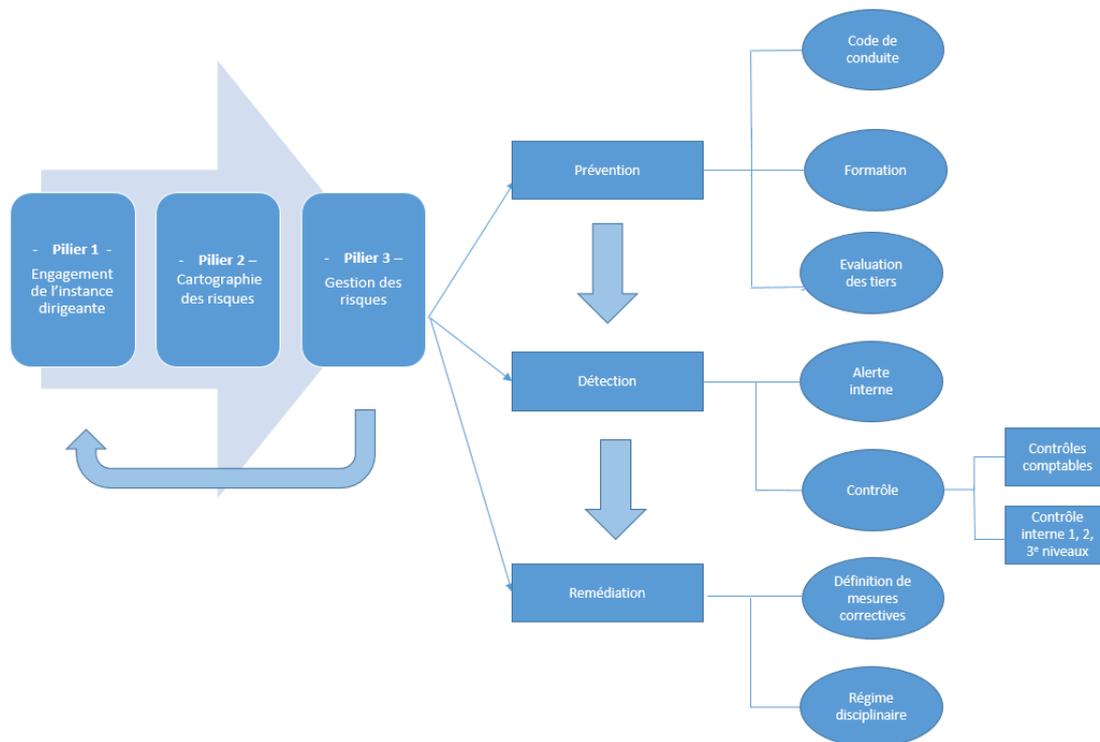
15. Les organisations qui exercent un contrôle sur d'autres entités s'assurent de la qualité et de l'efficacité du ou des dispositifs anticorruption déployés dans l'ensemble du périmètre qu'elles contrôlent.

2. Trois piliers indissociables

16. Un dispositif anticorruption repose sur trois piliers indissociables :

- premier pilier : l'engagement de l'instance dirigeante en faveur d'un exercice des missions, compétences ou activités de l'organisation exempt d'atteintes à la probité, ce qui suppose de sa part :
 - d'avoir un comportement personnel exemplaire, en paroles comme en actes, en matière d'intégrité et de probité ;
 - de promouvoir le dispositif anticorruption, par une communication personnelle ;
 - de mettre en œuvre des moyens suffisants pour permettre d'atteindre l'effectivité et l'efficacité du dispositif ;
 - d'être responsable du correct pilotage de ce dispositif ;
 - de s'y conformer pour la prise des décisions qui lui reviennent en propre ;
 - de s'assurer que des sanctions adaptées et proportionnées soient prononcées en cas de comportement contraire au code de conduite ou susceptible d'être qualifié d'atteinte à la probité ;
- deuxième pilier : la connaissance des risques d'atteintes à la probité auxquels l'entité est exposée, à travers l'élaboration d'une cartographie de ses risques ;
- troisième pilier : la gestion de ces risques, à travers la mise en œuvre de mesures et procédures efficaces tendant à leur prévention, à la détection d'éventuels comportements ou situations contraires au code de conduite ou susceptibles de constituer des atteintes à la probité et à la sanction de celles-ci. Cette gestion comprend également le contrôle et l'évaluation de l'efficacité desdites mesures et procédures.

Vue d'ensemble



Premier pilier : l'engagement de l'instance dirigeante

17. L'instance dirigeante s'entend des personnes placées à la tête de l'organisation et chargées de la gérer, en application de ses statuts et des normes en vigueur. Elle initie la démarche de mise en œuvre du dispositif anticorruption, valide sa conception et en assure le déploiement ainsi que le contrôle.

18. Lorsque l'instance dirigeante exerce ses fonctions sous le contrôle ou la surveillance d'un organe non exécutif, ce dernier veille à ce que les risques d'atteintes à la probité soient convenablement appréhendés par la mise en place d'un dispositif anticorruption adapté et efficace.

19. L'engagement de l'instance dirigeante en faveur d'un exercice des missions, compétences ou activités de l'organisation exempt d'atteintes la probité constitue un élément fondateur de tout dispositif anticorruption.

20. Cet engagement se manifeste non seulement par la volonté de l'instance dirigeante de prévenir et détecter toute atteinte à la probité au sein de son organisation, mais aussi par la mobilisation de moyens adaptés.

21. L'instance dirigeante déploie, selon des modalités adaptées et proportionnées au profil de risque de l'organisation qu'elle dirige, les moyens pour définir, mettre en œuvre et contrôler les mesures et procédures qui composent le dispositif anticorruption.

22. Elle est personnellement responsable de la conception, du déploiement et du contrôle du dispositif, même lorsqu'elle en confie la mise en œuvre à un collaborateur. Dans cette hypothèse, ce collaborateur doit être en mesure de lui rendre compte directement.

23. Elle s'assure que ce collaborateur, ainsi que les personnels qui l'assistent dans l'accomplissement de ses missions, disposent des connaissances nécessaires en raison de leur expérience ou de leur formation ainsi que d'un positionnement adéquat pour exercer leur mission et accéder aux informations nécessaires à l'exercice de leurs fonctions.

24. Elle s'assure également du bon fonctionnement du dispositif en place à travers l'examen des résultats des contrôles des différentes mesures et procédures du dispositif qui lui sont adressés.

25. L'instance dirigeante participe personnellement à la mise en œuvre opérationnelle de certaines mesures et procédures composant le dispositif anticorruption, à l'occasion, par exemple, de la validation de la cartographie des risques d'atteintes à la probité, de la prise de décision à l'issue de l'évaluation de certains tiers ou lorsqu'il s'agit de déterminer les sanctions à prononcer en cas de violation du code de conduite ou de faits susceptibles d'être qualifiés d'atteintes à la probité.

26. L'instance dirigeante communique sur son dispositif anticorruption en interne ainsi qu'en direction des tiers avec qui elle envisage d'entrer ou de demeurer en relation. Elle rappelle avec fermeté son engagement sans faille en faveur de l'éthique et de l'intégrité.

27. L'instance dirigeante s'assure que des sanctions adaptées et proportionnées sont prises en cas de violation avérée du code de conduite ou en présence de faits susceptibles d'être qualifiés d'atteintes à la probité.

Deuxième pilier : la cartographie des risques d'atteintes à la probité

28. La cartographie des risques d'atteintes à la probité constitue la pierre angulaire du dispositif anticorruption, car c'est sur son fondement que sont définies les autres mesures de prévention et de détection. Elle repose sur l'identification, l'évaluation et la hiérarchisation des risques d'atteintes à la probité propres à chaque organisation.

29. Elle participe d'une approche par les risques qui nécessite, d'une part, de comprendre et d'évaluer les risques d'atteintes à la probité auxquels l'organisation est exposée et, d'autre part, de prendre des mesures et procédures adaptées et proportionnées afin de les maîtriser efficacement.

30. La cartographie des risques prend la forme d'une documentation régulièrement actualisée, destinée à permettre à l'organisation de connaître les risques d'atteintes à la probité auxquels elle est exposée.

31. Issue d'une analyse fine des processus de l'organisation, la cartographie est établie sur le fondement d'une méthode offrant l'assurance raisonnable que les risques identifiés sont le fidèle reflet de ceux auxquels l'organisation est réellement exposée ; ces risques sont évalués à leur juste niveau, correctement hiérarchisés et couverts par des plans d'actions de nature à en assurer la maîtrise.

32. Cette cartographie est validée par l'instance dirigeante après, le cas échéant, avoir été présentée à l'organe non exécutif. Cette validation doit intervenir avant qu'elle ne soit mise en œuvre et lors de chacune de ses mises à jour.

33. La cartographie des risques peut être insérée dans une cartographie couvrant un spectre plus large de risques, qui respecte elle-même les dispositions énoncées aux paragraphes 28 à 32.

Troisième pilier : mesures et procédures de maîtrise des risques d'atteintes à la probité

Caractère systémique du dispositif anticorruption

34. La conception, le déploiement et la mise en œuvre du dispositif anticorruption doivent être adaptés aux risques préalablement identifiés, évalués et hiérarchisés par l'organisation.

35. Adaptées aux risques qu'elles ont pour objet de maîtriser, ces mesures et procédures s'articulent autour de trois objectifs : prévenir les risques, les détecter et, le cas échéant, remédier aux insuffisances constatées.

Mesures et procédures de prévention des atteintes à la probité

Le code de conduite et ses procédures/politiques annexes

36. Le code de conduite, ou tout document équivalent quelle que soit sa dénomination, précise les règles déontologiques applicables aux dirigeants, aux personnels, en définissant et illustrant, au regard de la cartographie des risques, les différents types de comportements à proscrire comme étant susceptibles de caractériser des atteintes à la probité.

37. Il est clair, sans réserve et sans équivoque.

38. Il est préfacé par l'instance dirigeante qui rappelle l'importance qu'elle attache à la lutte contre les atteintes à la probité au sein de l'organisation.

39. Dans le respect des normes applicables, le code de conduite est rendu opposable par tous moyens aux personnels de l'organisation. Lorsque l'organisation est dotée de règlement(s) intérieur(s), le code de conduite y est intégré, et fait l'objet, le cas échéant, de la procédure de consultation des instances, autorités ou services compétents.

40. D'autres politiques en matière de conduite éthique et de déontologie peuvent utilement y être intégrées ou lui être annexées, visant par exemple les cadeaux et invitations, le mécénat, le *sponsoring*, le *lobbying*, la gestion des conflits d'intérêts, les frais de représentation, les cumuls d'activités, ou toute autre procédure qui participe à la lutte contre les atteintes à la probité.

41. Le code de conduite et ses procédures et politiques annexes forment un ensemble cohérent, facilement accessible aux collaborateurs de l'organisation. Il peut utilement être communiqué aux tiers, le cas échéant, selon des modalités adaptées dans l'objectif de protéger les éventuelles informations confidentielles qu'il contient.

La sensibilisation et la formation aux risques d'atteintes à la probité

42. La sensibilisation de l'ensemble des personnels de l'organisation peut revêtir un caractère général.

43. Les cadres et les collaborateurs les plus exposés doivent, quant à eux, faire l'objet d'une formation obligatoire, adaptée à leurs métiers et aux risques auxquels ils peuvent être exposés. L'identification des bénéficiaires, comme le contenu de la formation, s'appuient sur la cartographie des risques d'atteintes à la probité.

44. Les collaborateurs bénéficiaires de cette formation doivent, à son issue, être en mesure de comprendre l'architecture du dispositif anticorruption, d'identifier les risques auxquels ils sont spécifiquement exposés dans l'exercice de leurs missions et les mesures et procédures applicables dans de telles situations. Ces objectifs doivent être atteints, quelles que soient les modalités de la sensibilisation et de la formation retenues.

45. Des indicateurs de suivi et des tests de connaissance sont par ailleurs définis pour permettre le pilotage de ces formations.

L'évaluation de l'intégrité des tiers

46. Si elle n'est pas suffisamment vigilante sur l'intégrité des tiers avec lesquels elle est entrée ou envisage d'entrer en relation, l'organisation peut se trouver impliquée, plus ou moins directement, dans la commission d'atteintes à la probité susceptibles de ternir sa réputation, d'avoir des conséquences défavorables sur le développement de ses activités, d'engager sa responsabilité ainsi que celle de son instance dirigeante.

47. Destinée à maîtriser ces risques, l'évaluation des tiers consiste à apprécier le risque que fait courir à l'organisation sa relation avec tel ou tel tiers, qu'il s'agisse de clients, de fournisseurs et prestataires, d'intermédiaires, de sous-traitants, de titulaires de marchés publics, de concessionnaires, de délégataires, de bénéficiaires de subventions, de cibles d'acquisitions, d'usagers, de partenaires, etc., c'est-à-dire avec toute personne physique ou morale avec laquelle elle est en relation et qui peut l'exposer à des risques potentiels d'atteintes à la probité.

48. La nature et la profondeur des évaluations à réaliser et des informations à recueillir sont prédéterminées en fonction des différents groupes homogènes de tiers, c'est-à-dire présentant des profils de risques comparables, tels que la cartographie des risques permet de les dresser. Ainsi, les groupes de tiers jugés pas ou peu risqués pourront ne pas faire l'objet d'une évaluation ou faire l'objet d'une évaluation simplifiée tandis que les groupes les plus risqués nécessiteront une évaluation approfondie.

49. Les évaluations peuvent être réalisées par différents moyens, allant d'une simple recherche en source ouverte à une enquête approfondie, en passant par l'envoi d'un questionnaire d'évaluation au tiers lui-même.

50. Les évaluations réalisées permettent à l'instance dirigeante d'apprécier l'opportunité d'entrer en relation avec un tiers, de poursuivre cette relation, le cas échéant avec des mesures de vigilance adaptées, ou de la rompre si elle est déjà engagée (1).

51. Les tiers en relation avec l'organisation qui présentent des risques élevés font l'objet de mesures de vigilance approfondies, de nature à sécuriser les opérations concernées. La surveillance des flux financiers et de l'accomplissement effectif et conforme des missions qui leur sont confiées y contribue notamment.

52. Dans le respect du cadre légal, des clauses spécifiques peuvent par ailleurs être insérées dans les contrats, prévoyant la rupture ou le non-renouvellement de la relation d'affaires en cas de survenance de faits susceptibles de constituer des atteintes à la probité ou de refus de se conformer aux directives de l'organisation en ce domaine.

Mesures et procédures de détection des atteintes à la probité

Le dispositif d'alerte interne

53. Le dispositif d'alerte interne permet le recueil des signalements de comportements ou de situations contraires au code de conduite ou susceptibles de constituer des atteintes à la probité.

54. Sans préjuger des éventuelles règles spécifiques à tel ou tel type d'organisations susceptibles d'influer sur leur dispositif d'alerte interne, celui-ci doit être adapté à la nature des risques de l'organisation et permettre à l'auteur de l'alerte d'effectuer de bonne foi son signalement, ainsi que de garantir sa protection.

55. La gestion de ce dispositif peut être réalisée au sein de l'organisation ou sous-traitée à un tiers, sous réserve que ce tiers dispose des compétences nécessaires au bon traitement des alertes et des moyens permettant d'en préserver la confidentialité.

56. Le dispositif d'alerte peut prévoir un ou plusieurs canaux de signalement allant de la simple adresse électronique dédiée, au logiciel de gestion voire, pour certaines organisations, à une plateforme éthique spécifique. Ils doivent être aisément accessibles aux agents ou collaborateurs de l'organisation, qu'ils soient ou non permanents. Les organisations peuvent utilement le rendre accessible aux tiers avec lesquels elles sont en relation.

57. Le dispositif d'alerte peut également prévoir que l'auteur du signalement en réfère prioritairement à son supérieur hiérarchique. Ce dernier doit pouvoir, le cas échéant, l'orienter et le conseiller, sauf s'il est lui-même l'auteur du comportement en cause.

58. Le dispositif d'alerte est sécurisé et les droits d'accès sont limités aux seuls personnels autorisés à recueillir les alertes ou à les traiter.

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

60. L'organisation définit les modalités de traitement des alertes qu'elle reçoit, et précise notamment :

- le référent fonctionnellement désigné pour recueillir les alertes au sein de l'organisation 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 de l'alerte, des faits objets de l'alerte et des personnes qui y sont visées, y compris lorsque des vérifications ou lorsque le traitement de l'alerte nécessitent la communication avec des tiers ;
- les modalités selon lesquelles l'auteur de l'alerte fournit, le cas échéant, les informations ou documents à l'appui de son alerte ;
- en cas d'enquête interne, les informations et documents professionnels susceptibles d'être exploités dans ce cadre ;
- les dispositions prises pour informer l'auteur de l'alerte de la réception et, le cas échéant, de la recevabilité de son alerte, ainsi que du délai nécessaire à son traitement et des suites qui lui sont réservées ;
- si aucune suite n'a été donnée à l'alerte, les dispositions prises pour détruire, dans les deux mois suivant la clôture des vérifications, les éléments du dossier permettant d'identifier l'auteur de l'alerte et les personnes mises en cause ;
- si un traitement automatisé des alertes est mis en place, les dispositions prises pour en assurer la conformité au regard des normes régissant la protection des données ;

- la mise en place d'indicateurs afin d'apprécier la qualité et l'efficacité du dispositif d'alerte (notamment : nombre d'alertes reçues, classées sans suite ou traitées, délais de traitement, problématiques soulevées). Ces indicateurs sont transmis à l'instance dirigeante ainsi que les signalements les plus sensibles.

Le dispositif de contrôle

61. L'organisation met en place un dispositif de contrôle et d'audit interne adapté et proportionné aux risques d'atteintes à la probité auxquels elle est exposée.

62. Ce dispositif répond à plusieurs objectifs :

- prévenir et détecter, le cas échéant, des atteintes à la probité ;
- contrôler la mise en œuvre effective, conforme et efficace des mesures et procédures de prévention et de détection des atteintes à la probité et définir des recommandations ou mesures correctives adaptées, en vue de leur amélioration.

63. Le dispositif de contrôle peut comprendre idéalement jusqu'à trois niveaux réalisés de façon autonome.

64. Le premier niveau de contrôle vise à s'assurer, au travers de contrôles préventifs réalisés avant que la décision ou l'opération ne soient mises en œuvre, que les tâches inhérentes à un processus opérationnel ou support ont été effectuées conformément aux procédures édictées par l'organisation. Les contrôles de premier niveau sont opérés par les équipes opérationnelles ou supports ou par la hiérarchie.

65. Les contrôles de deuxième niveau visent à s'assurer, au travers de contrôles détectifs conduits sur tout ou partie des décisions prises ou des opérations réalisées, selon une fréquence prédéfinie ou de façon aléatoire, de la bonne exécution des contrôles de premier niveau et du bon fonctionnement du dispositif anticorruption dans son ensemble.

66. Les contrôles de troisième niveau (ou « audits internes ») sont périodiques et visent à s'assurer que le dispositif de contrôle est conforme aux exigences de l'organisation, efficacement mis en œuvre et tenu à jour. Les personnes en charge des contrôles de troisième niveau sont indépendantes. Elles sont missionnées par l'instance dirigeante et lui rendent compte directement.

67. Les résultats des contrôles de deuxième et troisième niveaux et la mise en œuvre des mesures correctives sont régulièrement transmis à l'instance dirigeante.

68. L'organisation peut insérer son dispositif de contrôle et d'audit interne du dispositif anticorruption au sein d'un dispositif couvrant un spectre plus large de risques, sous réserve de respecter les dispositions énoncées aux paragraphes 61 à 67.

69. Parmi les procédures de contrôle et d'audit interne, les procédures de contrôle et d'audit comptable peuvent constituer un instrument privilégié de prévention et de détection des atteintes à la probité.

70. Les contrôles comptables consistent à s'assurer que les livres, registres et comptes ne sont pas utilisés pour masquer des faits d'atteintes à la probité. Ces procédures ciblent les situations à risques mises en évidence dans la cartographie des risques d'atteintes à la probité. En l'absence de tels contrôles, l'organisation les définit et les déploie.

71. Sans préjuger des éventuelles normes ou réglementations spécifiques à tel ou tel type d'organisation susceptibles d'influer sur leurs contrôles comptables, la séparation des responsabilités entre la vérification du service fait, la demande de mise en paiement, l'autorisation de mise en paiement et la mise en paiement effective contribue à la prévention des atteintes à la probité.

72. Idéalement, l'organisation met en place trois niveaux de contrôle comptable, selon les mêmes modalités que celles du contrôle interne, définies supra : les contrôles comptables de premier et second niveaux et les audits comptables.

73. Ces contrôles comptables peuvent être réalisés soit par les services de contrôle comptable et financier propres à l'organisation, soit par un auditeur externe disposant des compétences nécessaires à leur bonne réalisation.

74. L'organisation peut insérer son dispositif de contrôle et d'audit comptable destiné à prévenir et détecter les atteintes à la probité au sein d'un dispositif de contrôle et d'audit comptable général sous réserve de respecter les dispositions énoncées aux paragraphes 69 à 73.

La gestion des insuffisances constatées

75. Les insuffisances constatées à l'occasion, notamment, des contrôles réalisés, donnent lieu à la définition de mesures correctives, qui peuvent s'inscrire dans le cadre d'un plan d'actions.

76. Les plans d'actions ainsi définis rappellent les insuffisances constatées, détaillent les actions correctives à mener, désignent les personnes responsables de leur mise en œuvre et fixent les délais dans lesquels elles doivent y procéder.

77. L'état d'avancement de ces plans d'action fait l'objet d'un suivi régulier dont les résultats sont transmis à l'instance dirigeante.

78. En cas de non-respect du code de conduite ou de ses éventuelles annexes ou de survenance de faits susceptibles d'être qualifiés d'atteintes à la probité, l'instance dirigeante prend des sanctions adaptées aux comportements constatés.

79. Les sanctions prononcées sont recensées afin d'identifier leurs causes et d'éviter leur répétition.

80. L'instance dirigeante communique au sein de son entité sur les faits constatés et les sanctions ainsi prononcées, en respectant le principe de l'anonymat et en veillant à ce que les personnes sanctionnées ne soient pas aisément identifiables.

81. Lorsque l'instance dirigeante n'a pas, compte tenu de sa qualité, l'obligation de mettre en œuvre les dispositions de l'article 40 du code de procédure pénale en informant l'autorité de poursuite compétente des atteintes qui seraient de nature à constituer une infraction pénale, elle demeure libre de le faire si elle l'estime opportun, ainsi que de déposer plainte, le cas échéant.

Assurer la conservation et l'archivage des mesures et procédures et de leur méthode d'élaboration

82. Dans le respect des normes régissant la protection des données, et de celles relatives aux fichiers et aux libertés, l'organisation met en place un dispositif de conservation et d'archivage des documents et informations qui composent son dispositif anticorruption, afin d'en assurer l'auditabilité. Cette précaution est d'autant plus nécessaire lorsque les méthodes retenues par les organisations mentionnées au paragraphe 7 ne correspondent pas à celles proposées par les présentes recommandations.

83. Les méthodes suivies par l'organisation dans le cadre de l'élaboration de son dispositif anticorruption ou de ses mises à jour sont également conservées et archivées.

84. Ces documents et informations sont conservés selon des durées qui varient en fonction de la nature des informations contenues. En l'état de la législation et notamment du règlement général sur la protection des données (RGPD), une organisation ne peut pas conserver des données personnelles de manière illimitée. Les déclinaires des dispositions générales ci-dessous précisent ce point.

II. – Déclinaison des dispositions générales aux entreprises assujetties à l'article 17 de la loi

85. Les dispositions qui suivent déclinent et précisent, pour les entités soumises à l'article 17 de la loi, les dispositions énoncées aux paragraphes 13 à 84 des présentes recommandations.

86. En application du I de l'article 17 de la loi, les dirigeants des organisations énumérées au paragraphe 93, dénommées ci-après « entreprises », sont 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* ».

87. Les mesures et procédures énumérées au II de l'article 17 ne visent donc qu'à la prévention de deux des six infractions énumérées à 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.

88. Au-delà de ce que prévoit la loi, il est conseillé que le dispositif anticorruption d'une entreprise appréhende plus largement d'autres risques non expressément prévus par le texte, mais qui pourraient constituer les prémices ou la conséquence de ceux prévus par la loi ; c'est le cas en particulier des infractions de faux ou d'abus de biens sociaux qui justifient en particulier les contrôles comptables ou des infractions de recel ou de blanchiment de l'ensemble des faits visés à l'article 1 de la loi.

89. Sauf indication contraire, les infractions mentionnées au paragraphe 87 seront dénommées indistinctement « corruption » dans la suite du II des présentes recommandations.

90. Les sociétés d'économie mixte et les établissements publics industriels et commerciaux qui atteignent les seuils définis à l'article 17 restent aussi assujettis aux obligations définies par le 3° de l'article 3 de la loi. Par conséquent, au-delà des risques de corruption et de trafic d'influence, leur dispositif anticorruption doit impérativement couvrir les risques de concussion, de prise illégale d'intérêt, de détournement de fonds publics et de favoritisme.

91. Les entreprises qui exercent un contrôle 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 ou des dispositifs anticorruption déployés dans l'ensemble du périmètre qu'elles contrôlent.

II.1) Premier pilier : l'engagement de l'instance dirigeante

92. L'article 17 de la loi impose à l'instance dirigeante « (...) *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* ». A défaut, sa responsabilité peut être engagée devant la commission des sanctions de l'AFA. Il est donc dans son 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 de l'instance dirigeante

93. Constituent l'instance dirigeante, au sens du I de l'article 17 de la loi, les personnes suivantes :

- les présidents, les directeurs généraux et les gérants de sociétés 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 sociétés 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.

94. Un « groupe de sociétés » doit être entendu comme désignant l'ensemble formé par une société et ses filiales au sens de l'article L. 233-1 du code de commerce ou comme l'ensemble formé par une société et celles qu'elle contrôle au sens de l'article L. 233-3 du même code.

95. Si les membres des conseils d'administration ou autres organes de contrôle ou de surveillance ne sont pas visés, dans leur ensemble, par cette définition, ils s'assurent, dans le cadre de leur mission de surveillance des activités de l'entreprise, de l'existence, de la pertinence et de l'efficacité des mesures prises par les dirigeants afin de se conformer à leurs obligations légales. Pour ce faire, dans les sociétés dotées de tels organes, l'AFA recommande que le dispositif anticorruption et ses actualisations leur soient périodiquement présentés afin qu'ils disposent de toutes les informations nécessaires pour veiller à la conformité de l'entreprise à l'article 17 de la loi.

2. Responsabilité de l'instance dirigeante

96. L'instance dirigeante s'engage à mettre en œuvre une politique de tolérance zéro à l'égard de 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 de la corruption.

97. 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 un responsable de la conformité anticorruption, désigné ci-après « responsable de la conformité ».

98. L'instance dirigeante définit la stratégie de gestion des risques et s'assure de sa mise en œuvre. A cet égard, elle veille à formaliser l'approbation du dispositif et en particulier de la cartographie des risques de corruption. 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. 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.

99. Au-delà de la mise en œuvre des mesures et procédures qui composent le dispositif anticorruption, l'instance dirigeante est invitée à veiller à l'intégration de mesures anticorruption aux procédures et politiques à risque, au sein, par exemple, de sa gestion des ressources humaines, de sa politique commerciale ou d'achat :

- En matière de gestion des ressources humaines, l'instance dirigeante veille à ce que :
 - le processus de recrutement et de nomination des cadres et des personnels les plus exposés inclut l'évaluation de leur intégrité ;
 - les initiatives des managers pour promouvoir la prévention et la détection de faits de corruption auprès de leurs équipes sont encouragées et valorisées. Par exemple, le respect des mesures de prévention de la corruption peut être pris en compte dans la fixation de leurs objectifs annuels et l'évaluation de leur performance ;
- En matière de politique commerciale, l'instance dirigeante est invitée à veiller à ce que l'octroi de remises commerciales, rabais et ristournes aux clients ne soit pas utilisé à des fins corruptives ;
- La mise en concurrence des fournisseurs participe enfin de la maîtrise des risques inhérents à la fonction achats.

100. L'instance dirigeante s'assure qu'un régime disciplinaire est mis en place et que des sanctions adéquates soient prises en cas de faits de corruption.

3. Moyens dédiés

101. La mise en œuvre d'un dispositif anticorruption nécessite des moyens humains et financiers proportionnés au profil de risque de l'entreprise, mis à disposition par l'instance dirigeante.

102. Ces moyens doivent couvrir notamment :

- l'équipe chargée de la conformité anticorruption ;
- le recours à des conseils ou prestataires externes, le cas échéant ;
- la mise en place d'outils 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 conformité

103. La désignation du responsable de la 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, qui tiennent compte des choix stratégiques et organisationnels retenus et des caractéristiques de l'entreprise (notamment : modèle économique, secteur d'activité, taille) ;

- les éléments qui garantissent l'indépendance du responsable de la 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 anticorruption dans l'entreprise, notamment les moyens matériels et humains qui y sont consacrés.

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

105. 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 conformité au niveau central et des référents par exemple par filiale, par pays ou par unité opérationnelle.

106. 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 de méthodologies et de politiques communes, à adapter le cas échéant en fonction des contraintes locales (taille, risques propres identifiés, options retenues dans l'organisation de la fonction conformité, réglementations, etc.).

107. Le responsable de la 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 du ou des dispositifs anticorruption. Ce réseau, qui facilite notamment la remontée de questions et, le cas échéant, d'alertes ainsi que des retours d'expérience, participe à l'amélioration du ou des dispositifs anticorruption de l'entreprise.

108. L'instance dirigeante veille à ce que le responsable de la conformité bénéficie à tout moment de :

- un accès à toute information utile à l'exercice de ses fonctions, lui permettant de disposer d'une image fidèle de l'activité de l'entreprise ;
- l'indépendance de son action vis-à-vis des autres fonctions de l'entreprise et la capacité à influencer réellement sur ces dernières ;
- un accès à l'instance dirigeante, afin d'en obtenir l'écoute et le soutien.

109. Indépendamment de son positionnement dans l'organigramme, il est primordial que le responsable de la conformité entretienne un lien direct et régulier avec l'instance dirigeante, ainsi qu'un accès facilité au conseil d'administration.

110. Au-delà de ses missions récurrentes, le responsable de la conformité est associé à la mise en œuvre des projets stratégiques et aux prises de décisions structurantes de l'entreprise, tels que, par exemple, la conclusion de nouveaux contrats, les fusions-acquisitions, les investissements majeurs, la prospection ou la constitution d'un partenariat, la conception et la commercialisation de nouveaux produits ou services.

111. L'indépendance du responsable de la conformité ne signifie pas pour autant l'absence de contrôle. A cet effet, il rend compte à l'instance dirigeante de son activité.

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

- de la capacité à exercer une fonction transverse ;
- 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.

Une politique de communication interne et externe adaptée

113. L'entreprise communique largement sur sa politique de prévention et de détection de la corruption, auprès de l'ensemble de son personnel.

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

115. L'entreprise communique également, selon des modalités adaptées, sa politique anticorruption aux partenaires extérieurs, dans l'objectif de protéger son personnel de sollicitations indues.

II.2) Deuxième pilier : la cartographie des risques

116. Aux termes du 3° du II de l'article 17 de la loi, la cartographie des risques « [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. »

117. 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, etc.) qu'elles ont aussi pour objet de prévenir et de détecter le trafic d'influence.

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

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

- de disposer d'une connaissance étendue 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 apporte une assurance raisonnable que la cartographie reflète fidèlement les risques auxquels l'entreprise est réellement exposée lorsqu'elle interagit avec des tiers. Chaque entreprise établit sa propre cartographie des risques, qui lui est spécifique, et ne peut en conséquence être appliquée en l'état à une autre entreprise ;
- d'identifier les rôles et responsabilités des acteurs concernés de l'entreprise, quel que soit leur niveau.

1. Objectifs de la cartographie des risques

120. 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.

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

121. La cartographie des risques 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 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

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

- d'une part, elle couvre les processus managériaux, opérationnels et support mis en œuvre par les entreprises dans le cadre de leurs interactions avec leurs tiers. Elle appréhende les risques de corruption en prenant en compte les particularités de chaque entreprise, notamment : secteurs d'activité, zones géographiques, contexte concurrentiel et réglementaire, typologies de tiers, modèle de revenus, chaîne de valeur, métiers et processus, organisation interne de l'entreprise, circuits de décision ;
- 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. A cet effet, celles-ci communiquent leur cartographie des risques de corruption et les plans d'actions associés à la maison-mère qui en suit périodiquement la réalisation. Ces cartographies peuvent utilement être agrégées au sein de celle de l'entreprise-mère. Cette dernière a ainsi une vision globale des risques encourus par ses différentes entités et des plans d'action associés.

124. La cartographie des risques est formalisée, c'est-à-dire qu'elle prend la forme d'une documentation écrite et structurée, qui décrit en détail les méthodes retenues pour son élaboration, les mesures prises pour maîtriser les risques, ainsi que les rôles et responsabilités des différentes personnes parties prenantes.

125. En fonction des activités et de l'organisation de l'entreprise, la cartographie peut être organisée, par exemple, par métier, par processus, par entité ou par zone géographique.

126. La cartographie des risques doit être un outil de pilotage des risques ; elle doit également faciliter l'appréciation, par des personnes extérieures à l'entreprise, de la pertinence du dispositif anticorruption (notamment en cas de contrôle administratif ou de procédure judiciaire).

127. 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. A 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

128. 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. La description fait ressortir l'impact potentiel 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.

129. Dans ce contexte, afin d'identifier, d'évaluer et de gérer les risques de corruption, il est recommandé de respecter les étapes ci-après.

130. Pour les entreprises ayant déjà conduit des travaux de cartographie des risques dans un cadre plus large ou sur d'autres types de risques que ceux de corruption, ces démarches préexistantes peuvent être capitalisées.

1^{re} étape : rôles et responsabilités des parties prenantes
à la cartographie des risques

131. Au sein des entreprises, les rôles et responsabilités peuvent utilement être 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 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 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 conformité est chargé d'établir la cartographie des risques de corruption, qu'il communique à l'instance dirigeante à chacune de ses mises à jour ainsi que le suivi du plan d'actions.
- les responsables des processus décisionnels, opérationnels, comptables et autres activités support contribuent, tous et chacun à leur place, à l'élaboration et à la mise à jour de la cartographie des risques. Ils sont responsables de l'identification des risques spécifiques à leurs activités conformément aux procédures anticorruption en vigueur dans l'entreprise.
- le responsable en charge de la maîtrise des risques, quand l'entreprise en dispose, 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 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, etc.) 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.

132. 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, y compris celles des dirigeants, des administrateurs et des gérants.

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

133. 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 sur la base des activités qu'elle exerce, le cas échéant sur le fondement d'une cartographie des processus préexistante. A ce stade, 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 ;
- dans une seconde étape et sur la base du recensement des processus, l'entreprise organise des échanges, notamment au moyen d'ateliers, d'entretiens, de l'envoi de questionnaires, avec des personnels de tous niveaux hiérarchiques et issus de l'ensemble de l'entreprise. Ces personnels sont choisis pour leur maîtrise opérationnelle de ces processus, afin d'identifier les 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 notamment.

134. Il s'agit de procéder à un état des lieux précis permettant d'identifier, de manière circonstanciée et documentée, les scénarios de risques propres à l'entreprise. Si une liste de risques pré établie peut constituer un des supports sur lesquels s'appuie la réflexion menée lors des échanges susmentionnés, elle ne saurait pré déterminer la nature, le nombre et la classification des scénarios de risque retenus à l'issue des échanges.

135. Ces échanges permettent la libre expression des participants et font l'objet de synthèses écrites qui précisent notamment l'ensemble des scénarios et facteurs de risque identifiés.

136. Les scénarios de risques sont identifiés en tenant compte de l'environnement dans lequel s'inscrit l'entreprise, qui peut notamment être affecté par :

- les pays dans lesquels l'entreprise déploie ses activités ;
- les secteurs d'activité ;
- la nature des opérations, notamment les d'opérations stratégiques (opérations de fusions-acquisitions, cessions d'actifs, association avec un nouveau partenaire stratégique, etc.) ;
- la nature du tiers, son secteur d'activité, la nature des relations (directe ou indirecte), la présence de personnes politiquement exposées, le degré de dépendance économique ;

- la durée du cycle de vente et la pression concurrentielle, les modalités de rémunération des commerciaux ;
- les conditions et les moyens de paiement ;
- l'historique des incidents constatés au sein de l'entreprise : doivent notamment être pris en compte les incidents que les audits internes ou le dispositif d'alerte interne ont permis de révéler, qui ont, le cas échéant, donné lieu à l'application du régime disciplinaire ;
- les faits ayant donné lieu à des décisions juridictionnelles concernant des entreprises aux risques comparables.

3^e étape : évaluation des risques bruts

137. 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.

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

139. 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 naturellement cumuler plusieurs types d'impacts.

140. 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).

141. 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.

142. Les échanges organisés pour identifier les risques peuvent utilement conduire à leur évaluation. Qu'elle s'appuie ou pas sur ces échanges, 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.

4^e étape : évaluation des risques nets ou résiduels

143. 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.

144. Il convient, à ce stade d'élaboration de la cartographie, d'évaluer l'efficacité des mesures de maîtrise des risques existantes en s'appuyant notamment sur les audits réalisés.

145. Idéalement, le recensement des moyens de maîtrise des risques déjà existants et mis en œuvre est réalisé à l'occasion des échanges avec le personnel, conduits dans le cadre de l'identification des risques inhérents aux activités de l'entreprise (2^e étape). L'évaluation de l'efficacité de ces mesures et ce faisant des risques nets ou résiduels est faite par le responsable de la conformité, en lien si nécessaire avec les responsables des fonctions de l'entreprise concernées et avec l'appui éventuel de l'audit interne et du responsable de la maîtrise des risques, quand l'entreprise possède une telle fonction.

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

146. Une fois les risques « nets » ou « résiduels » évalués, un classement par niveau des scénarios de risques apparaît.

147. Lorsque ces scénarios de risques présentent une évaluation nette de même niveau et si l'entreprise juge utile de les départager pour prioriser les actions à mettre en œuvre, elle peut les hiérarchiser au moyen d'une méthode objective adaptée à ses activités spécifiques, 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.

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

149. 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.

150. Sur la base de ces éléments, un plan d'actions est élaboré. Son calendrier et ses modalités de mise en œuvre, 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 constituent une condition de l'efficacité de la cartographie des risques.

6^e étape : formalisation, mise à jour et archivage de la cartographie des risques

151. 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.

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

153. La mise à jour de la cartographie peut opportunément permettre à l'entreprise d'adapter sa méthodologie ou d'adopter une nouvelle méthodologie pour que la cartographie qui en sera issue offre l'assurance raisonnable que les risques identifiés reflètent fidèlement les risques auxquels elle est réellement exposée, soient évalués à leur juste niveau et correctement hiérarchisés.

154. Il convient de conserver les éléments suivants, qui permettent d'apprécier la mise en œuvre effective de la cartographie :

- la trace des échanges avec les personnels concernés (calendriers, notes, synthèses écrites) ;
- la méthode de calcul des risques « *bruts* », ainsi que les définitions retenues ;
- la méthode de calcul des risques « *nets* » ou « *résiduels* », ainsi que les définitions retenues ;
- Les procédures d'identification et de classification des risques ;
- 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.

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

II.3) Troisième pilier : la gestion des risques

A. – Prévention des risques

1. Code de conduite

156. Le 1^o 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

157. Le code de conduite, 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.

158. 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.

Champ d'application et communication

159. Le code de conduite est applicable et opposable à l'ensemble des personnels de l'entreprise.

160. 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 conseillé 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 variées avec des risques de corruption spécifiques, il peut être opportun pour l'entreprise de décliner son code de conduite au niveau de ses entités ou de ses unités opérationnelles.

161. Les autres collaborateurs amenés à travailler avec l'entreprise et qui sont soumis à son règlement intérieur doivent respecter le code de conduite.

162. S'agissant des tiers, le code de conduite peut utilement leur être communiqué, sous réserve d'adaptations rendues nécessaires pour protéger les éventuelles informations confidentielles qu'il contient. Il est recommandé d'imposer aux tiers le respect de ce document, par une clause contractuelle.

Processus d'élaboration et de validation

163. Le code de conduite est préparé conjointement par le responsable de la conformité et les personnes qualifiées de l'entreprise.

164. Il est validé par l'instance dirigeante qui en assure le portage, par exemple en préfaçant son introduction. 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.

165. L'instance dirigeante promeut le code de conduite et en applique scrupuleusement les principes. Son exemplarité est essentielle à la bonne appropriation et application du code de conduite par les personnels.

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

166. 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.

167. 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

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

169. 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 par l'entreprise et dont elle devra conserver la trace.

Contenu

170. Le code de conduite a vocation à être rédigé postérieurement à l'élaboration de la cartographie des risques, dans la mesure où il décrit les comportements à proscrire à partir des risques identifiés.

171. 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.

172. Le code de conduite est accompagné d'illustrations pertinentes sur des cas concrets.

173. 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. A ce titre, il peut traiter notamment des cadeaux et invitations, des paiements de facilitation, des conflits d'intérêts, du mécénat, du sponsoring ainsi que, le cas échéant, de la représentation d'intérêts (*lobbying*) et des frais de représentation.

174. Le code de conduite présente le dispositif d'alerte interne destiné à recueillir les signalements relatifs à l'existence de conduites ou de situations contraires à ses dispositions.

175. 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 font l'objet de sanctions disciplinaires.

176. Le code de conduite mentionne la fonction qualifiée pour répondre aux questions des personnels (par exemple : responsable de la conformité, référent conformité ou intégrité) et les modalités pour la contacter (notamment adresse générique).

177. Le code de conduite 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 Etats étrangers.

Mise à jour

178. L'opportunité de mettre à jour le code de conduite est examinée régulièrement et notamment après une mise à jour de la cartographie. Il comporte à cette fin une indication de date d'effet.

2. Sensibilisation et formation

179. Conformément au 6^o 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.* ».

180. Le dispositif de formation anticorruption s'adresse donc à l'ensemble des cadres, en tant que personnels chargés d'un certain niveau de responsabilité dans l'entreprise, ainsi qu'aux autres membres du personnel de l'entreprise considérés comme les plus exposés aux risques de corruption.

Définition et objectifs

181. Vecteur des valeurs et de la culture d'intégrité au sein de l'entreprise, un dispositif de formation efficace et adapté favorise une large diffusion des engagements pris par l'instance dirigeante en matière de lutte contre la corruption, ainsi que leur appropriation par les collaborateurs concernés. Il peut utilement s'inscrire dans un dispositif plus large de sensibilisation de l'ensemble du personnel.

182. Si le dispositif de sensibilisation permet aux bénéficiaires d'être mieux informés et réceptifs sur les sujets qui leur sont présentés, le dispositif 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.

183. Le dispositif de formation anticorruption doit :

- être coordonné avec les autres mesures et procédure du dispositif anticorruption. Par exemple : 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 personnels

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

185. Les actions de sensibilisation peuvent porter notamment sur :

- le code de conduite, traduction de l'engagement de l'instance dirigeante ;
- la corruption en général, ses enjeux, ses 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.

186. 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

187. La formation des cadres et des 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 risque. Elle vise à ce qu'ils s'approprient le dispositif anticorruption de l'entreprise.

188. A terme, la formation a pour effet de limiter les risques identifiés dans la cartographie des risques.

189. Les personnels les plus exposés sont identifiés à partir de la cartographie des risques. Il peut s'agir, en particulier :

- des personnels en relation avec certains tiers (notamment : commerciaux, acheteurs) ;
- des personnels qui participent à la mise en œuvre du dispositif anticorruption.

190. 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.

191. 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.

192. La formation a pour objectif d'améliorer la compréhension et la 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 induite ;
- des sanctions disciplinaires encourues en cas de pratiques non conformes.

193. Le tronc commun de ces formations porte sur :

- le code de conduite, traduction de l'engagement de l'instance dirigeante ;
- 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.

194. 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 de la corruption peuvent être une thématique couverte par la formation à destination des personnels chargés d'une fonction de contrôle.

195. Les cadres et les personnels les plus exposés sont formés au cours de leur parcours d'intégration. Les formations sont ensuite régulièrement dispensées tout au long de l'exercice de leur activité.

196. A l'instar du code de conduite, les formations s'appuient notamment sur des cas pratiques et des scénarios personnalisés par public et adaptés aux risques identifiés dans la cartographie des risques.

197. Des personnels 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.

198. 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 connaissances peut être effectué au cours de la formation et passé un certain délai, afin de s'assurer que les connaissances ont bien été assimilées.

Contrôle et suivi du dispositif de formation

199. 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.

200. Le responsable de la conformité doit être informé du calendrier des formations et de leur contenu pédagogique, mais doit aussi pouvoir contrôler le déploiement du dispositif et les indicateurs associés.

3. Evaluation de l'intégrité des tiers

201. Le 4^o 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

202. La loi impose aux entreprises de procéder à l'évaluation des clients, des fournisseurs de premier rang et des intermédiaires.

203. Il est également recommandé d'inclure dans les dispositifs d'évaluation d'autres catégories de tiers avec lesquels l'entreprise peut être en relation ou vouloir entrer en relation, notamment : ses cibles d'acquisition, ses bénéficiaires d'action de *sponsoring* ou de mécénat.

204. Les évaluations visent à permettre de décider d'entrer ou pas en relation avec un tiers, de poursuivre une relation en cours ou d'y mettre fin.

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

205. Les évaluations des tiers 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).

206. Elles peuvent néanmoins être mises en œuvre à travers un dispositif unique, pour autant que ce dernier permette de faire ressortir le risque spécifique de corruption.

Définition des modalités d'évaluation des tiers

207. 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 dresser. Ainsi, les groupes de tiers jugés pas ou peu risqués pourront ne pas faire l'objet d'une évaluation ou faire l'objet d'une évaluation simplifiée, tandis que les groupes les plus risqués nécessiteront une évaluation approfondie.

208. L'entreprise peut recenser de manière exhaustive ses tiers. Cette approche a pour objet de déterminer *ex ante*, sur le fondement de la cartographie des risques, les groupes de tiers qui lui semblent les plus sensibles aux risques de corruption.

209. Au sein de chaque groupe de tiers qui nécessite une évaluation, chacun 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.

210. 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. Un tiers, considéré comme appartenant à un groupe peu risqué peut être requalifié en tiers risqué à l'issue de son évaluation individuelle. Par ailleurs, un incident, une alerte, une condamnation concernant un tiers dont le groupe est jugé peu risqué ou dont le comportement évolue au cours de la relation peuvent conduire l'entreprise à réaliser une évaluation plus poussée ou à l'évaluer en priorité.

211. Une base de données interne dédiée aux tiers, conforme à la réglementation, peut utilement être mise en place. Elle doit être sécurisée et à jour. 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.

Modalités d'évaluation de l'intégrité des tiers

212. Trois niveaux d'acteurs participent aux évaluations :

- le personnel en charge des évaluations collecte les informations et documents utiles à l'évaluation des tiers avec lesquels l'entreprise est ou est appelée 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.

213. 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 nécessaires, ou lorsque le tiers réside ou intervient dans un pays où elle n'est pas implantée. Au regard des objectifs assignés par la loi, l'entreprise demeure responsable de la qualité et de la pertinence des évaluations réalisées pour son compte.

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

215. 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.

216. A 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.

217. 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.

218. L’entreprise identifie les noms, prénoms des principaux actionnaires, ainsi que des bénéficiaires effectifs.

219. L’entreprise apprécie la sensibilité du secteur d’activité du tiers au regard du risque de corruption. 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.

220. L’entreprise s’assure que le tiers - en particulier s’il s’agit d’un intermédiaire ou un fournisseur- dispose de l’expérience, des qualifications et des compétences nécessaires à la réalisation de sa mission. A 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.

221. L’entreprise recherche si le tiers, ses dirigeants, ses principaux actionnaires et ses bénéficiaires effectifs 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).

222. Les informations sont obtenues, dans le respect des réglementations applicables, notamment celles relatives à la protection des données personnelles.

223. 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 point de vigilance.

224. 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

225. 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.

226. 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.

227. 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. 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.

228. 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.

229. L’entreprise s’assure, en particulier pour les prestataires ou intermédiaires, que le recours à ces tiers est justifié et que leur prestation est effective.

230. L’entreprise identifie les raisons qui conduisent à choisir un tiers plutôt qu’un concurrent de ce tiers. Par exemple, constitue une alerte pour une entreprise le fait que le tiers soit recommandé ou imposé par un client.

231. Le versement de commissions liées à l’obtention de contrats peut constituer un facteur de risque lors de l’évaluation du niveau de risque du tiers.

232. 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 Etat figurant dans la liste des Etats et territoires non coopératifs).

233. 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.

234. Si le tiers n'est pas implanté sur le territoire français ou si la prestation est réalisée à l'étranger, son évaluation prend en compte la sensibilité du pays au risque de corruption, à partir :

- 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 lutte contre la corruption d'agents publics étrangers dans les transactions commerciales internationales dans les pays signataires ;
- d'enquêtes ou d'indices publiés relatifs à la corruption dans le secteur public ;
- de l'enregistrement du tiers dans un Etat 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.

235. 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.

236. 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, elle peut avoir intérêt à s'assurer que les tiers avec lesquels elle est liée effectuent l'évaluation de leurs propres tiers conformément aux paragraphes précédents.

Conclusions à tirer des évaluations des tiers

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

238. A 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).

239. Les personnes à l'origine de la décision ainsi que les modalités de prise de décision sont clairement identifiées dans l'entreprise.

240. L'absence de facteurs de risque en suite d'évaluation ne garantit pas que la relation avec le tiers soit absolument dénuée de risque. A 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 à déployer en cours de relation d'affaires

241. 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.

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

- informer le tiers de l'existence de son dispositif anticorruption en communiquant, par exemple, le code de conduite ;
- former ou sensibiliser le tiers au risque de corruption ;
- 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 ;
- inciter le tiers à vérifier l'intégrité de ses propres sous-traitants afin de sécuriser la chaîne contractuelle.

Suivi de la relation contractuelle avec le tiers

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

244. A cet égard, l'entreprise doit avoir une visibilité complète sur les paiements reçus de tiers ou effectués à leur profit 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, une délégation de paiement au profit d'un tiers ou un changement de domiciliation 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

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

246. Les informations sur la situation du tiers qui n'impactent pas le niveau de risque de l'entreprise donnent lieu à une mise à jour des informations sur le tiers. En revanche, si ces informations portent sur 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, alors une nouvelle évaluation du tiers est conduite.

247. Le processus de réévaluation 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

248. Un suivi du dispositif d'évaluation des tiers est mis en place et peut comprendre :

- 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, révélant des cas non conformes.

249. 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 à tout autre responsable désigné.

Conservations des informations sur les tiers

250. 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.

B. – Détection

1. Dispositif d'alerte interne

251. 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

252. Le dispositif d'alerte interne est la procédure mise en œuvre par les entreprises afin de permettre notamment 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 (cf. annexe 1).

Articulation des différents dispositifs d'alerte

253. Différents dispositifs d'alerte professionnelle, prévus par des textes spécifiques, coexistent, il est conseillé, dans un souci de lisibilité, la mise en place d'un dispositif technique unique de recueil des signalements, qui feront l'objet de traitement approprié.

254. 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).

255. Un signalement qui porte sur des atteintes à la probité et témoigne d'une défaillance du dispositif de conformité pourra être adressé à l'AFA.

Organisation du dispositif d'alerte

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

257. Le dispositif d'alerte interne 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.

258. 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.

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

260. La gestion de ce dispositif (y compris la fonction de référent définie ci-dessous) peut être sous-traitée à un tiers, sous réserve qu'il 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.

261. Le dispositif d'alerte est à déployer sur l'ensemble du périmètre des entités contrôlées par l'entreprise.

Traitement des alertes

262. 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.

263. 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.

264. 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.

265. 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.

266. 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 transmis par l'auteur de l'alerte et susceptibles d'être exploités ;
- 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.

267. 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.

268. 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.

269. Les alertes peuvent être adressées de manière anonyme. Le dispositif doit permettre une poursuite des échanges avec l'auteur de l'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).

270. 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 pourra prévoir notamment :

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

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

272. 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.

273. Toute enquête interne est diligentée par une ou plusieurs personnes qualifiées, désignées par l'instance dirigeante de l'entreprise.

274. L'instance dirigeante est au minimum informée des enquêtes ouvertes relatives aux situations les plus sensibles, à l'exception de celles où elle est elle-même mise en cause.

275. A 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.

276. Lorsque les soupçons apparaissent suffisamment étayés, ce rapport est communiqué à l'instance dirigeante (où à l'organe de contrôle lorsque cette dernière est mise en cause) afin qu'elle décide des suites à donner.

277. 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 ou son délégataire.

278. Enfin, une action judiciaire peut 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 tenue de le faire si elle relève des autorités énumérées à l'article 40 du code de procédure pénale.

279. 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).

Mise en œuvre du dispositif d'alerte interne

280. Les étapes suivantes peuvent utilement être observées :

- établissement d'une procédure formalisée qui peut notamment prévoir la désignation d'un référent alerte et la mise en place d'un comité intégrant des personnes qualifiées, soumises à des obligations de confidentialité renforcée. Ce comité assure une prise de décision collégiale sur les suites à réserver aux alertes reçues ;
- présentation du 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, etc.) 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, etc.) ;
- 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 niveaux 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 ;
- mise en place d'indicateurs 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, etc.). Ces indicateurs sont transmis à l'instance dirigeante.

Archivage des alertes et de leur traitement

281. 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.

282. 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.

283. 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.

284. 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, 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'Etat.

2. Le contrôle interne

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

285. 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.

286. 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 (5) visent à s'assurer 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 supports ou par le responsable hiérarchique ;
- les contrôles de deuxième niveau (6) visent à s'assurer, selon une fréquence prédéfinie ou de façon aléatoire, de la bonne exécution des contrôles de premier niveau. Les contrôles de deuxième niveau peuvent être réalisés par le responsable de la conformité, une fonction qualité, la fonction de gestion des risques, le contrôle de gestion notamment ;
- 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.

287. 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 utilement permettre à l'entreprise de couvrir plus largement les risques identifiés à travers la cartographie des risques de corruption.

288. 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 ;

– et d'évaluer les dispositifs de contrôle en place de nature à maîtriser ces risques.

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

- couvre les situations à risque 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.

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

291. 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

292. 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.

293. 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

294. 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

295. Les entreprises disposent 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.

296. 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 (par exemple, 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.

297. Ils sont établis au regard des situations à risques mises en évidence dans la cartographie des risques de corruption, parmi les contrôles généraux existants, par approfondissement ou en complément de ceux-ci.

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

- les opérations telles que le sponsoring, le mécénat, les honoraires et les commissions, les frais de représentation et de déplacement, les cadeaux et invitations, les dons, les legs, etc. ;
- les flux atypiques (par exemple, les comptes d'attente ou transitoires) ;
- les opérations exceptionnelles ou à enjeu ;
- les opérations liées au recours à des tiers relevant d'un groupe présentant un niveau de risque élevé tels que des intermédiaires ou des consultants ;
- les flux financiers ou de matière vers des comptes ou des tiers relevant d'un groupe 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.

299. 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

300. 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

301. 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).

302. 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 différent de celui qui en a effectué la saisie.

303. 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.

304. 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.

305. 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.

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

307. 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.

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

309. 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.

310. 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 niveaux.

Traitement des anomalies constatées

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

312. 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 en coordination avec le responsable de la conformité.

313. 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.

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

Externalisation

315. 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, etc.) que l'entreprise mobilise à cette fin ;
- en externe, par les entités que l'entreprise mandate à cette fin.

316. 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 audité, à la prévention et à la détection de la corruption. Il est rappelé qu'il est tenu de révéler au procureur de la République les faits présumés délictueux – y compris donc les faits de corruption - dont il a connaissance au cours de sa mission.

C. – Contrôle et évaluation du dispositif anticorruption

1. Objectifs et modalités

317. 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.

318. 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.

319. Ces contrôles peuvent s'articuler autour des trois niveaux de contrôle susmentionnés.

320. Le responsable de la conformité élabore un plan de contrôle de deuxième niveau couvrant l'ensemble du dispositif anticorruption.

321. 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 conservation des pièces afférentes aux contrôles.

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

323. 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 anticorruption 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.

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

2. Typologie de contrôles à déployer

325. 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.

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

	327. Cartographie des risques de corruption
Contrôles de 1^{er} niveau :	Les contrôles liés à la cartographie ne peuvent être réalisés qu'après son établissement et ses mises à jour. Aucun contrôle de premier niveau ne peut être réalisé dans ce cadre.
Contrôles de 2^e niveau :	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 3^e 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.
	328. Code de conduite

Contrôles de 1^{er} niveau :	- Validation 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 2^e 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 3^e 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.

	329. Formation
Contrôles de 1^{er} niveau :	- Vérification de la présence des collaborateurs concernés et des connaissances qu'ils ont acquises lors des formations.
Contrôles de 2^e 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 3^e 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/à distance...) 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.

	330. Évaluation des tiers
Contrôles de 1^{er} niveau :	- Contrôle 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 2^e 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 3^e 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.
	331. <u>Alerte interne</u>
Contrôles de 1^{er} 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 2^e niveau :	- Contrôle régulier de la correcte réalisation des contrôles de premier niveau, sur la base d'un échantillonnage représentatif de dossiers.
Contrôles de 3^e 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.
	332. <u>Contrôles comptables</u>
Contrôles de 1^{er} 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 2^e 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 3^e 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.
	333. <u>Régime disciplinaire</u>
Contrôles de 1^{er} niveau :	Le contrôle de la conformité du régime disciplinaire ne peut être effectué qu'une fois les sanctions prononcées.
Contrôles de 2^e niveau	- Contrôle, pour chaque incident, de la prise de sanction ; - Vérification de l'adéquation entre l'incident et la sanction.
Contrôles de 3^e 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.

334. Si l'entreprise a déployé au sein de son dispositif anticorruption d'autres mesures et procédures en complément de 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.

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

336. 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.

337. 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.

D. – Remédiation

1. Gestion et suivi des insuffisances constatées

338. 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.

2. Régime disciplinaire

Définition

339. 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 comme fautif.

340. 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

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

Mécanisme

342. Lorsque des manquements aux devoirs d'intégrité et de probité des personnels sont constatés, une procédure disciplinaire est engagée à leur encontre et des sanctions proportionnées leurs sont infligées.

343. 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.

Recensement des sanctions

344. L'entreprise peut utilement recenser les sanctions disciplinaires prononcées à l'encontre des personnels de l'entité, ce qui favorise le renforcement des mécanismes de maîtrise des risques d'atteintes à la probité.

345. 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

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.

III. – Déclinaison des dispositions générales aux acteurs publics assujettis au 3° de l'article 3 de la loi

346. Les dispositions qui suivent déclinent et précisent, pour les acteurs publics soumis au 3° de l'article 3 de la loi, les dispositions énoncées aux paragraphes 13 à 84 des présentes recommandations.

347. La loi donne compétence à l'Agence française anticorruption pour contrôler « *la qualité et l'efficacité des procédures mises en œuvre au sein des administrations de l'Etat, des collectivités territoriales, de leurs établissements publics et sociétés d'économie mixte, et des associations et fondations reconnues d'utilité publique pour prévenir et détecter les faits de corruption, de trafic d'influence, de concussion, de prise illégale d'intérêt, de détournement de fonds publics et de favoritisme* ». Le législateur a créé l'obligation pour les entités ainsi définies (ci-après dénommées « acteurs publics »), de déployer un dispositif anticorruption.

348. Les présentes recommandations visent à faciliter la réalisation par les acteurs publics des objectifs définis par la loi en proposant les modalités de mise en œuvre d'un dispositif anticorruption.

349. La spécificité des acteurs publics en matière de prévention et de détection des atteintes à la probité réside dans la grande diversité de leurs missions, compétences, statuts juridiques, structures de gouvernance, territoires, des normes d'intégrité qui les régissent, du statut de leurs collaborateurs, des différentes catégories de tiers avec lesquels ils interagissent et de leur taille. Il s'ensuit que les acteurs publics sont invités à mettre en œuvre les recommandations d'une façon proportionnée à leur profil de risques. Ils peuvent tout autant recourir à d'autres méthodes permettant d'atteindre les mêmes résultats.

350. Ces recommandations ne détaillent pas l'ensemble des dispositions obligatoires qui s'appliquent aux acteurs publics et qui concourent à la prévention et à la détection des atteintes à la probité, en raison à la fois de leur nombre et de la variété des régimes juridiques applicables aux différentes catégories d'acteurs publics. Toutefois, les recommandations comprennent des focus sur des points particuliers concernant un grand nombre d'acteurs publics.

351. Les acteurs publics qui exercent un contrôle sur d'autres entités (par exemple : fondations, filiales, entreprises publiques locales, établissements publics, etc.) s'assurent de la qualité et de l'efficacité du ou des dispositifs anticorruption déployés dans l'ensemble du périmètre qu'ils contrôlent. A ce titre, ils peuvent choisir soit d'élaborer eux-mêmes le dispositif anticorruption applicable aux entités qu'ils contrôlent (par exemple, pour celles qui sont de taille modeste), soit de mettre en place des procédures et un contrôle interne visant à s'assurer de la qualité et de l'efficacité du ou des dispositifs anticorruption déployés dans l'ensemble du périmètre qu'ils contrôlent.

352. Le dispositif anticorruption de l'acteur public concerne, outre ses agents et collaborateurs, les membres de l'instance dirigeante, l'ensemble des élus qui ne font pas partie de l'instance dirigeante et les membres des cabinets ainsi que, si nécessaire, les bénévoles contribuant à ses activités.

III.1) Premier pilier : l'engagement de l'instance dirigeante

353. Les obligations qui imposent aux acteurs publics de mettre en place des procédures pour prévenir et détecter les atteintes à la probité procèdent non seulement de la loi (7), mais également, pour la plupart d'entre eux, de diverses dispositions législatives et réglementaires. Il s'agit notamment, pour les acteurs publics qui emploient des agents publics, des obligations déontologiques (obligations de déclaration d'intérêts ou de situation patrimoniale pour certains élus et cadres dirigeants, obligation de déport ou d'abstention en cas de conflit d'intérêts, encadrement des cumuls d'activités, prévention des conflits d'intérêts lors des cessations de fonction, obligation de désignation d'un référent déontologue, etc.) (8). D'autres dispositions concourent également à la réduction des risques d'atteintes à la probité comme celles du code général des collectivités territoriales sur le fonctionnement des assemblées délibérantes, les règles de la commande publique et le décret n° 2012-1246 du 7 novembre 2012 modifié relatif à la gestion budgétaire et comptable publique.

354. Il incombe donc à l'instance dirigeante de veiller à ce que ces dispositions soient connues des personnes concernées et réellement mises en œuvre. A défaut, sa responsabilité administrative ou pénale pourrait être engagée.

355. Toutefois, la mise en œuvre de ces dispositions législatives et réglementaires ne permet pas, à elle seule, de disposer d'un dispositif complet et efficace de prévention et de détection des atteintes à la probité. Aussi ces recommandations ont-elles pour objectif d'aider les acteurs publics à élaborer un tel dispositif.

1. Définition de l'instance dirigeante

356. Constitue l'instance dirigeante les personnes – élues ou nommées – disposant de compétences et de pouvoirs propres pour gérer un acteur public, en application de ses statuts et des textes législatifs et réglementaires en vigueur.

357. Il s'agit notamment des personnes ou instances suivantes :

- pour les services de l'Etat : ministre, secrétaire général, directeur d'administration centrale, autorité préfectorale, responsable de services déconcentrés ;
- pour les collectivités territoriales : organe exécutif (maire, président de conseil départemental, de conseil régional, de conseil territorial, d'assemblée, etc.), président d'établissement public de coopération intercommunale (EPCI), ainsi que le directeur général des services ;
- pour les établissements publics, sociétés d'économie mixte : président du conseil d'administration et directeur ;
- pour les établissements publics de santé : directeur ;
- pour les fondations reconnues d'utilité publique, selon l'organisation qu'elles ont choisie : président du conseil de surveillance, président du directoire, président du conseil d'administration ainsi que directeur ;
- pour les associations reconnues d'utilité publique : président et directeur.

358. Ces instances disposent d'un pouvoir d'organisation de l'entité ou du service, d'allocation des moyens et de représentation de l'entité, qui leur confère un rôle déterminant dans la mise en place d'un dispositif anticorruption.

2. Responsabilité de l'instance dirigeante

359. L'instance dirigeante s'engage à mettre en œuvre une politique de tolérance zéro envers tout comportement qui pourrait contrevenir au devoir de probité, promeut et diffuse la culture de la probité au sein de l'acteur public et vis-à-vis des tiers, en érigeant la prévention et la détection des atteintes à la probité à un niveau prioritaire.

360. La responsabilité de la mise en place du dispositif anticorruption repose sur l'instance dirigeante qui peut, le cas échéant, et sans s'affranchir de sa responsabilité personnelle, en déléguer la mise en œuvre opérationnelle à un collaborateur ou un service.

361. Quelle que soit l'organisation retenue, le délégataire doit disposer d'un positionnement lui assurant l'autonomie et la légitimité nécessaires à la conduite de sa mission. Ce positionnement doit faciliter un accès direct à l'instance dirigeante.

362. 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. A cet égard, elle veille à formaliser l'approbation de ce dispositif, et en particulier de la cartographie des risques d'atteintes à la probité. Elle s'assure de l'élaboration d'un plan d'actions y afférent et de la mise à disposition des moyens adaptés pour l'exécuter et en assurer le suivi régulier.

363. L'instance dirigeante s'assure que le respect des mesures de prévention et de détection des atteintes à la probité est pris en compte dans la fixation des objectifs annuels et l'évaluation de la performance de l'encadrement. Les initiatives de l'encadrement pour promouvoir la prévention et la détection des atteintes à la probité auprès de ses équipes doivent être valorisées.

364. 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.

365. La mise en œuvre des mesures et procédures qui composent le dispositif anticorruption induit pour l'instance dirigeante d'intégrer des mesures de maîtrise des risques aux procédures et politiques publiques exposées de son organisation, notamment la gestion des ressources humaines, la commande publique et l'attribution de subventions publiques.

366. L'instance dirigeante prend, dans le respect des normes applicables (droit du travail, statut de la fonction publique) les sanctions disciplinaires adéquates en cas de comportements constitutifs d'une atteinte à la probité, d'un manquement au code de conduite ou d'un manquement au devoir de probité.

367. L'instance dirigeante veille à ce que les entités que contrôle l'acteur public (en droit ou en fait) soient couvertes par un dispositif anticorruption.

368. L'instance dirigeante veille à ce que le dispositif anticorruption lui soit applicable.

369. Lorsque l'instance dirigeante exerce ses fonctions sous le contrôle ou la surveillance d'un organe non exécutif ou d'une tutelle, ces derniers veillent à ce que les risques d'atteintes à la probité soient appréhendés par la mise en place d'un dispositif anticorruption adapté et efficace.

3. Moyens dédiés

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

371. La désignation du collaborateur ou du service chargé de la mise en œuvre opérationnelle du dispositif de prévention et de détection peut faire l'objet d'une communication spécifique à l'ensemble des personnels et, le cas échéant, être formalisée par une lettre de mission de l'instance dirigeante précisant notamment :

- les missions confiées ;
- les éléments qui garantissent son autonomie, tels que son positionnement dans l'organigramme et les modalités d'accès à l'instance dirigeante ;
- l'articulation avec les autres fonctions de l'acteur public ;
- les moyens matériels et humains affectés ou susceptibles d'être mobilisés.

372. L'instance dirigeante s'assure que ce collaborateur ou ce service dispose des moyens et des compétences lui permettant de réaliser ses missions, de coordonner les fonctions concernées et de rendre compte à l'instance dirigeante.

373. Son positionnement dans la structure doit lui garantir :

- un accès à toute information utile pour disposer d'une image fidèle de l'activité de l'acteur public ;
- l'indépendance de son action vis-à-vis des autres fonctions et la capacité à influencer réellement sur ces dernières ;
- un accès aisé à l'instance dirigeante, afin d'en obtenir l'écoute et le soutien.

374. Indépendamment de son positionnement dans l'organigramme, il entretient un lien direct et régulier avec l'instance dirigeante.

4. Une politique de communication interne et externe adaptée

375. L'instance dirigeante communique sur sa politique de prévention et de détection des atteintes à la probité, ainsi que sur le dispositif global qui la matérialise auprès de l'ensemble des élus, du personnel et des tiers (usagers, fournisseurs, prestataires, associations, partenaires).

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

III.2) Deuxième pilier : la cartographie des risques d'atteintes à la probité

377. Indispensable instrument de la connaissance des risques d'atteintes à la probité, la cartographie des risques permet aux acteurs publics d'engager et de formaliser une réflexion en profondeur sur leurs risques ainsi que 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 la réalisation des risques.

378. Cette cartographie peut être spécifique ou intégrée dans une cartographie générale des risques, sous réserve de l'utilisation d'une méthodologie offrant l'assurance raisonnable que les risques d'atteintes à la probité identifiés, évalués et hiérarchisés soient le fidèle reflet des risques auxquels l'acteur public est réellement exposé.

379. La cartographie des risques des acteurs publics vise la maîtrise des risques de l'ensemble des infractions d'atteintes à la probité énumérées à l'article 1^{er} de la loi.

380. Pour les acteurs publics relevant à la fois de l'article 3 et de l'article 17 de la loi (soit les établissements publics industriels et commerciaux et les SEM dont le chiffre d'affaires et les effectifs atteignent les seuils fixés par l'article 17), la cartographie doit intégrer les risques relatifs à l'ensemble des infractions d'atteintes à la probité énumérées à l'article 1 de la loi.

381. L'établissement de la cartographie des risques d'atteintes à la probité nécessite :

- de disposer d'une connaissance précise de l'acteur public et de ses activités, dont les processus (9) que celles-ci nécessitent de mettre en œuvre. Cette connaissance est la condition préalable à l'analyse fine des processus qui garantit que la cartographie des risques d'atteintes à la probité reflète fidèlement les risques auxquels l'acteur public est réellement exposé. Chaque acteur public établit sa propre cartographie des risques, qui lui est spécifique et ne peut en conséquence être transposée en l'état à un autre acteur public ;
- nécessite d'identifier les rôles et responsabilités des acteurs concernés à tous les niveaux de l'organisation.

1. Objectifs de la cartographie des risques d'atteintes à la probité

382. La cartographie des risques d'atteintes à la probité donne à l'instance dirigeante la connaissance nécessaire pour la mise en œuvre de mesures de prévention et de détection efficaces, proportionnées aux enjeux identifiés par la cartographie et adaptées aux activités de l'acteur public concerné.

383. Deuxième pilier du dispositif de prévention et de détection, la cartographie des risques d'atteintes à la probité permet à l'acteur public de gérer efficacement ses risques en identifiant les mesures et procédures de prévention, de détection et de remédiation à mettre en place. Réciproquement, les enseignements tirés de la mise en œuvre de ces mesures et procédures sont pris en compte pour établir et mettre à jour la cartographie des risques d'atteintes à la probité. L'ensemble de ces interactions s'inscrit ainsi dans une approche systémique de la cartographie des risques et des mesures et procédures conçues et mises en œuvre pour les gérer.

2. Caractéristiques de la cartographie des risques d'atteintes à la probité

384. La cartographie des risques est complète dans la mesure où elle couvre :

- tout d'abord, l'ensemble des acteurs, y compris les élus, les ministres, les membres des différents cabinets, les comptables publics, les contrôleurs généraux économiques et financiers, ainsi que l'ensemble des agents, quel que soit leur statut (agents titulaires, agents contractuels, agents détachés ou mis à disposition, personnels sous contrat de droit privé, vacataires, apprentis, stagiaires, bénévoles) ;
- ensuite, « de bout en bout », les processus managériaux, opérationnels et support mis en œuvre par l'acteur public dans le cadre de ses activités. Résultant de l'analyse de l'ensemble des processus de l'acteur public, ainsi que de l'identification des risques d'atteintes à la probité, et ce à chaque stade de ces processus, elle appréhende ces risques en prenant en compte les particularités de chaque acteur public : missions, compétences, spécialité, structure de gouvernance et circuits de décision, statut des personnels, territoires, typologies de tiers, ressources propres, etc. ;
- enfin, l'entier périmètre d'intervention de l'acteur public, soit l'ensemble des structures, notamment les entités qu'il contrôle. Si le choix a été fait de laisser tout ou partie des structures contrôlées réaliser par elles-mêmes leurs cartographies des risques d'atteintes à la probité, l'acteur public s'assure de leur existence et de la pertinence des méthodes choisies pour les établir.

385. La cartographie des risques d'atteintes à la probité 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.

386. Au choix de l'acteur public, la documentation peut être organisée, par exemple, par compétence, par processus, par entité ou par territoire. 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 d'atteintes à la probité.

387. La cartographie des risques est évolutive puisqu'il est nécessaire de réévaluer les risques de manière périodique, en particulier chaque fois qu'évolue un élément important de l'acteur public. A la faveur de son actualisation, la cartographie participe d'un processus d'amélioration continue permettant aux acteurs publics de renforcer la maîtrise de leurs risques.

3. Les différentes étapes de mise en place d'une cartographie des risques d'atteintes à la probité

388. La cartographie des risques d'atteintes à la probité procède d'une analyse objective, structurée et documentée des risques auxquels un acteur public est exposé 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.

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

390. Pour les acteurs publics ayant déjà conduit des travaux de cartographie des risques, par exemple des risques opérationnels, stratégiques, budgétaires ou comptables ou en matière de gestion des fonds européens, ces démarches préexistantes peuvent être capitalisées, sous réserve que la méthode employée pour les construire soit conforme aux préconisations qui suivent. En effet, la cartographie des risques d'atteintes à la probité relève d'une méthode analogue : l'acteur public a d'ores et déjà procédé à une description de tout ou partie de ses processus et il dispose d'une expérience en matière d'identification et de cotation des risques, ainsi que dans la détermination d'une stratégie de maîtrise des risques. Les scénarios de risque déjà identifiés au titre des risques opérationnels, stratégiques, budgétaires ou comptables ou en matière de gestion des fonds européens peuvent ainsi être examinés et enrichis, lorsque cela est pertinent, des risques d'atteintes à la probité qu'ils recèlent. Ce procédé ne garantit toutefois pas que les scénarios de risque ainsi identifiés reflètent fidèlement les risques d'atteintes à la probité auxquels l'organisation est réellement exposée. L'usage de la méthode basée sur l'analyse des processus exposée *infra* est de nature à utilement compléter cette approche.

1^{re} étape : rôles et responsabilités des parties prenantes à la cartographie des risques d'atteintes à la probité

391. Au sein des acteurs publics, les rôles et responsabilités peuvent utilement être répartis comme suit :

- l'instance dirigeante promeut l'exercice de cartographie des risques et donne les moyens de sa mise en œuvre au collaborateur ou au service auquel elle en a confié l'élaboration. Elle valide la stratégie de gestion des risques mise en œuvre sur son fondement et s'assure de l'exécution du plan d'actions retenu ;
- le collaborateur ou service responsable coordonne l'élaboration de la cartographie des risques, en accompagnant les services dans le recensement des processus, dans l'identification des risques d'atteintes à la probité, dans l'évaluation et la hiérarchisation de ces risques et dans la définition et la mise en œuvre de mesures concourant à leur maîtrise. Il communique la cartographie des risques à l'instance dirigeante 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 en rendant compte des risques spécifiques au périmètre relevant de leur responsabilité ;
- les personnels, forts de leur expérience pratique des processus de l'acteur public, apportent leur contribution à l'exercice de cartographie en rendant compte des facteurs spécifiques aux fonctions exercées et aux risques encourus.

392. L'acteur public, 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 (y compris les bénévoles et les stagiaires), ainsi que ceux attachés aux missions des dirigeants, des élus et de leurs collaborateurs.

2^e étape : identification des risques inhérents aux activités de l'acteur public (recensement des processus et scénarios de risques)

393. L'identification des risques de l'acteur public s'appuie sur une analyse fine de ses processus :

- dans une première étape, l'acteur public établit un recensement de ces processus, le cas échéant sur le fondement d'une cartographie des processus préexistante. Lors de ce premier recensement, l'acteur public 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. Dans le cas d'un acteur public ne disposant d'aucune bibliothèque de processus, le recensement pourra, dans une première étape, cibler les macro-processus auxquels sera appliquée la méthodologie décrite aux paragraphes qui suivent. Cette première étape doit être suivie d'une revue à une échelle plus fine des processus et des scénarios de risques associés ;
- dans une seconde étape et sur la base du recensement des processus, l'acteur public organise des échanges (ateliers, entretiens individuels, etc.) avec des personnels de tout niveau hiérarchique et de toutes les fonctions de l'acteur public, choisis pour leur maîtrise opérationnelle de ces processus. Ces échanges permettent la libre expression des participants et font l'objet de comptes rendus écrits.

394. Ces échanges ont pour objet d'identifier, par processus, des scénarios de risques (10) auxquels l'acteur public est exposé dans le cadre de ses activités et de certains métiers. Il ne s'agit pas de décliner la typologie théorique des risques auxquels il est exposé, 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'acteur public doit en effet fonder sa cartographie sur la réalité de ses processus.

395. La cartographie des risques intègre l'intervention des tiers de l'acteur public, qui peut présenter un risque d'exposition à une sollicitation (facteur de risque).

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

- le fonctionnement interne de l'acteur public et notamment sa gouvernance ;
- son organisation territoriale, notamment les administrations déconcentrées, les opérateurs de l'Etat ;
- les « liens d'intérêts » de l'instance dirigeante et des personnels ;
- la nature des tiers avec lesquels l'acteur public interagit, à l'occasion par exemple des achats auxquels il procède, des aides et subventions qu'il attribue ou des autorisations qu'il délivre, ainsi que des secteurs d'activité du tiers, la nature de la relation (directe ou indirecte), le degré de dépendance économique, etc. ;
- l'historique des incidents : doivent être pris en compte notamment les incidents ayant affecté l'acteur public, révélés par les audits internes ou par les dispositifs d'alerte interne et déontologique, les faits ayant donné lieu à l'application du régime disciplinaire ou à des décisions juridictionnelles concernant des acteurs publics similaires, les observations de la Cour des comptes et de la chambre régionale des comptes, le retour d'expérience tiré du contrôle de légalité.

3^e étape : évaluation des risques bruts

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

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

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

400. 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).

401. L'appréciation des facteurs jugés aggravants est réalisée par l'application de coefficients de gravité. Par exemple, dans la situation des acteurs publics 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.

402. Les échanges organisés pour identifier les risques peuvent utilement permettre de procéder à l'évaluation des risques bruts identifiés. Qu'elle s'appuie ou pas sur ces échanges, l'évaluation des risques bruts est conduite sur le fondement d'une méthodologie homogène. L'acteur public veille notamment à ce que les évaluations des risques bruts émanant de ses différentes composantes puissent être agrégées de manière cohérente.

4^e étape : évaluation des risques nets ou résiduels

403. Cette étape vise à évaluer le niveau de maîtrise des risques par l'acteur public 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.

404. 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.

405. *Nota.* – Dans le cas d'une cartographie des risques « intégrée », conduisant à évaluer le niveau de risque d'un scénario ou d'un processus en agrégeant différentes natures de risque, dont le risque d'atteintes à la probité, il conviendra de s'assurer que cette évaluation fasse ressortir la cotation de ce risque en tant que tel.

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

406. Une fois les risques « nets » ou « résiduels » évalués, un classement par niveau des scénarios de risques apparaît.

407. Lorsque ces scénarios de risques présentent une évaluation nette de même niveau, et si l'acteur public juge utile de les départager pour prioriser les actions à mettre en œuvre, il convient de les hiérarchiser au moyen d'une méthodologie objective adaptée aux activités spécifiques de l'acteur public, reposant sur la combinaison de plusieurs critères comme la part du budget consacré, la nature et le type de relations avec les tiers.

408. 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.

409. 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 constituent une condition de l'efficacité de la cartographie des risques.

410. Les acteurs publics pas ou peu familiers des exercices de cartographie des risques peuvent utilement, dans leur cheminement tendant à se doter d'une cartographie des risques d'atteintes à la probité, telle que proposée dans les précédents paragraphes, débiter leurs travaux en examinant prioritairement trois processus que l'expérience conduit à considérer comme particulièrement exposés aux risques d'atteintes à la probité : la commande publique, la gestion des ressources humaines, le versement des subventions (cf. annexe n° 2).

6° étape : formalisation, mise à jour et archivage de la cartographie des risques d'atteintes à la probité

411. L'ensemble des éléments précités constitue la cartographie des risques. Sa présentation participe de son appropriation comme outil de pilotage des risques d'atteintes à la probité.

412. La nécessité d'une éventuelle actualisation de la cartographie doit être appréciée chaque année.

413. Cette mise à jour doit suivre la méthode ayant conduit à la construction de la cartographie, si celle-ci 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'acteur public est exposé.

414. Il est recommandé de conserver tous les éléments permettant d'apprécier la mise en œuvre effective des modalités et méthodologies de la cartographie.

415. Les différentes versions des cartographies sont datées, référencées et archivées.

III.3) *Troisième pilier : la gestion des risques d'atteintes à la probité*

A. – Prévention des risques

1. Règles en matière de déontologie/éthique et code de conduite

Définition et objectifs du code de conduite

416. Le code de conduite, quelle que soit la dénomination retenue, est un document qui manifeste la décision de l'instance dirigeante d'engager l'acteur public dans une démarche de prévention et de détection des atteintes à la probité. Il peut être intégré dans un dispositif « d'éthique » (du type charte éthique) ou de déontologie au périmètre plus large que la stricte prévention des atteintes à la probité, à condition d'en permettre la parfaite lisibilité dans sa présentation et sa diffusion.

417. Le code de conduite définit et illustre, à travers des exemples d'activités de l'acteur public, les différents types de comportements à éviter comme étant susceptibles de constituer des atteintes à la probité.

Champ d'application

418. Le code de conduite est applicable à l'ensemble des personnels et dirigeants de l'acteur public, ainsi que, le cas échéant, sous une forme adaptée, aux autres élus et à leurs collaborateurs.

419. Concernant les autres collaborateurs de l'acteur public (bénévoles, stagiaires), il est recommandé que le code leur soit également applicable, dans le respect des dispositions légales qui les concernent.

Processus d'élaboration et de validation

420. 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.

421. Le code de conduite, préfacé par l'instance dirigeante, rappelle ses valeurs et son engagement en matière de prévention et de détection des atteintes à la probité. Ce portage favorise le développement d'une culture de la déontologie, de l'éthique, de l'intégrité et de la probité.

422. Pour ce qui concerne les acteurs publics dont les personnels relèvent du statut général des fonctionnaires, le code de conduite est signé par le chef de service. Il requiert la consultation préalable du comité technique ou, à l'avenir, du comité social compétent.

423. Lorsque l'acteur public est doté de règlement(s) intérieur(s), le code de conduite y est intégré, et fait l'objet, le cas échéant, de la procédure de consultation des instances, autorités ou services compétents.

Contenu

424. Le code de conduite a vocation à être rédigé ou mis à jour postérieurement à l'élaboration de la cartographie des risques d'atteintes à la probité, dans la mesure où il décrit les comportements à éviter à partir des risques spécifiques à l'acteur public.

Le code de conduite n'est pas limité à un recueil de bonnes pratiques, mais contient des dispositions sur les types de comportements à éviter auxquels personnels et dirigeants sont susceptibles d'être confrontés du fait de l'activité de l'acteur public. Une structuration en rubriques correspondant aux différents types de comportements à éviter est encouragée.

425. Par ailleurs, le code de conduite rappelle et précise les modalités de mise en œuvre des obligations déontologiques applicables au personnel et aux dirigeants de l'acteur public.

426. Certaines de ces obligations peuvent être d'origine législative ou réglementaire. Le code de conduite peut apporter des précisions quant à leur mise en œuvre opérationnelle. En outre, ces obligations peuvent être utilement complétées par des mesures propres à l'acteur public, en fonction de son profil de risque (11).

427. Le code de conduite traite notamment des cadeaux et invitations, des conflits d'intérêts, des règles d'utilisation des biens du service, des frais de représentation et peut ainsi détailler :

- les obligations d'intégrité et de probité cités à l'article 25 du titre I^{er} du statut général des fonctionnaires et à l'article 1^{er} de la loi n° 2013-907 du 11 octobre 2013 relative à la transparence de la vie publique, pour les responsables publics ;
- les dispositions spécifiques à certaines catégories d'agents (forces de sécurité intérieure, secteur médico-social), dès lors qu'elles sont représentées au sein de l'acteur public ;
- les dispositions relatives aux déclarations d'intérêts et de situation patrimoniale applicables dans l'acteur public ;
- le cadre applicable en matière de cumul d'activités, de mobilité des agents publics vers le privé et de retour dans le service public d'agents en mobilité dans le secteur privé ;
- toutes règles applicables en matière de prévention des conflits d'intérêts : obligation de déport, voire dispositifs volontaires de déclaration de non-conflit d'intérêts ou de déclaration d'intérêts ;
- l'interdiction des emplois familiaux dans les cabinets des élus, si l'acteur public est concerné ;
- les règles applicables au cumul de fonctions électives et administratives ;
- l'obligation de gestion par un intermédiaire agréé des instruments financiers pour certains emplois ou fonctions ;
- les obligations de transparence et de communicabilité des documents applicables dans la gestion de l'acteur public.

428. Le code de conduite est appuyé d'illustrations pertinentes au regard de l'activité de l'acteur public et des risques définis dans sa cartographie des risques d'atteintes à la probité (par exemple, quel comportement adopter en cas d'invitation par un fournisseur ou par une personne ayant formulé une demande de délivrance de titre ou d'autorisation).

429. Si l'acteur public fait le choix d'un code de conduite renvoyant à des fiches ou procédures « opérationnelles » 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 ces documents constituent un ensemble cohérent, clairement articulé et dont la lisibilité et l'accessibilité soient assurées pour tous les collaborateurs.

430. Le code de conduite mentionne le nom et les coordonnées du référent déontologue (lorsqu'il en existe un) et celles du référent alerte, qui peuvent le cas échéant être les mêmes. Afin d'éviter une confusion entre ces deux instances, le code de conduite précise leurs rôles respectifs et leurs procédures de saisine.

431. Il présente le dispositif d'alerte interne destiné à recueillir les signalements relatifs à l'existence de comportements ou de situations contraires au code de conduite et susceptibles, pour les agents relevant du statut général des fonctionnaires, de constituer un manquement au devoir de probité.

432. Le code de conduite rappelle que les violations de ses dispositions sont susceptibles de faire l'objet de sanctions disciplinaires dans le respect des dispositions applicables.

433. Pour ce qui concerne les personnels relevant du statut général des fonctionnaires, les manquements aux mesures d'organisation du service et de son activité prévues dans le code de conduite sont susceptibles de donner lieu à une sanction disciplinaire. Les manquements aux obligations déontologiques légales rappelées par le code de conduite sont également susceptibles de donner lieu à une sanction disciplinaire. Enfin, les manquements aux préconisations du code de conduite intervenant dans le domaine statutaire sont eux aussi susceptibles de donner lieu à une sanction disciplinaire dès lors qu'ils sont constitutifs d'un manquement aux devoirs de probité et d'intégrité des agents publics. Le manquement aux préconisations du code de conduite est un indice de l'existence d'un manquement aux devoirs de probité et d'intégrité.

Formalisation et accessibilité du code de conduite

434. Le code de conduite, rédigé en des termes qui le rendent intelligible et accessible à des non spécialistes est clair, sans réserve et sans équivoque.

435. Le code de conduite est communiqué en interne et constitue l'un des éléments auxquels sont formés les personnels et les dirigeants de l'acteur public.

436. Le code de conduite sert également d'outil de communication externe dans les relations avec les usagers, les fournisseurs, et, plus généralement, les partenaires de l'acteur public concerné.

Mise à jour

437. Le code de conduite est mis à jour régulièrement, notamment après la mise à jour de la cartographie des risques d'atteintes à la probité. Il comporte à cette fin une indication de sa date d'établissement.

2. Formation et sensibilisation

Définition et objectifs

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

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

440. 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'acteur public.

441. Le dispositif de sensibilisation et de formation doit :

- être coordonné avec les autres mesures et procédures du dispositif anticorruption. Par exemple : formation au contenu du code de conduite, formation prioritaire des personnes identifiées comme à risque sur le fondement de la cartographie des risques, 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 personnels

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

443. Les actions de sensibilisation, destinées à tous les personnels, portent notamment sur :

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

444. Quelles que soient les modalités d'organisation retenues, ces actions de sensibilisation visent à favoriser la prise de conscience des enjeux inhérents aux atteintes à la probité au sein de l'acteur public et son environnement.

Formation obligatoire destinée aux personnes les plus exposées

445. La formation de l'instance dirigeante, des élus et de leurs collaborateurs, 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 risque.

446. Cette formation vise à ce que les personnes concernées s'approprient le dispositif anticorruption de l'acteur public.

447. A terme, elle a pour effet de limiter les risques identifiés dans la cartographie des risques d'atteintes à la probité.

448. Sur le fondement de celle-ci, le responsable des ressources humaines identifie, avec l'aide de l'éventuel responsable ou service en charge du dispositif anticorruption (ou tout autre responsable désigné), les personnes les plus exposées aux risques d'atteintes à la probité, c'est-à-dire les personnes en charge ou participant aux processus à risque.

449. Il peut s'agir, en particulier :

- de l'instance dirigeante et des élus (notamment ceux titulaires d'une délégation) ;
- des cadres et des personnels en relation avec des tiers exposés (acheteurs, instructeurs de demandes de subventions ou d'autorisations, etc.) ;
- des personnels qui participent à la mise en œuvre du dispositif anticorruption.

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

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

452. Ce contenu est adapté à la nature des risques, aux fonctions exercées et aux territoires sur lesquels intervient l'acteur public. Il est actualisé régulièrement, en lien avec la mise à jour de la cartographie des risques.

453. La formation a pour objet d'améliorer la compréhension et la 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 induite ;
- des sanctions disciplinaires encourues en cas de pratiques non conformes.

454. Le tronc commun de ces formations porte sur :

- le code de conduite ;
- les atteintes à la probité en général, leurs enjeux et leurs formes ;
- les obligations juridiques applicables et les sanctions y afférentes ;
- le dispositif anticorruption ;
- le comportement à adopter, le rôle et les responsabilités de chacun face à des faits d'atteintes à la probité ;
- le dispositif d'alerte interne.

455. 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.

456. Les personnes les plus exposées sont formées dès leur prise de fonction. Les formations sont régulièrement dispensées tout au long de l'exercice de leur fonction.

457. Les formations sont mises en œuvre avec des outils adaptés. Elles doivent être accessibles et adaptées aux publics auxquels elles s'adressent.

458. Les formations sont pragmatiques et pédagogiques. A l'instar du code de conduite, elles s'appuient notamment sur des cas pratiques et des scénarios personnalisés par public et adaptés aux risques identifiés dans la cartographie des risques d'atteintes à la probité.

459. Des membres de l'acteur public peuvent être invités à 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.

460. 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 ou après un certain délai, afin de s'assurer que les connaissances ont été assimilées.

461. Les formations peuvent être assurées par des personnels en interne ou être dispensées par un prestataire extérieur.

462. Dans l'hypothèse d'une externalisation, il est nécessaire que l'acteur public participe à la conception et à la mise en œuvre de la formation afin que ses spécificités soient prises en compte et que le contenu de la formation soit en cohérence avec la politique déployée en la matière (ex. : éléments relatifs au code de conduite, à la cartographie des risques...).

463. Enfin, les atteintes à la probité peuvent également être abordées dans le cadre de formations plus générales (commande publique, management, prise de poste à responsabilité, formation des élus...).

Contrôle et suivi du dispositif de formation

464. 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 le dispositif de prévention et de détection des atteintes à la probité.

465. La qualité du dispositif de formation et son suivi, ainsi que l'identification des participants font l'objet d'un contrôle.

466. Dans l'hypothèse d'une externalisation de tout ou partie du dispositif de formation, le collaborateur ou le service responsable du dispositif anticorruption (ou tout autre responsable désigné) doit non seulement être informé du calendrier des formations et de leur contenu pédagogique, mais doit aussi contrôler le déploiement effectif du dispositif et les indicateurs associés.

3. L'évaluation de l'intégrité des tiers

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

467. Les évaluations sont réalisées à partir de la cartographie des risques d'atteintes à la probité. Elles peuvent concerner notamment les catégories de tiers suivantes : les fournisseurs et les sous-traitants, les entités que l'acteur public subventionne, les bénéficiaires d'aides individuelles, les bénéficiaires d'autorisations, les partenaires ou mécènes, les usagers du service public, tout acteur privé ou public avec lequel l'acteur public est en relation dans le cadre de ses missions, y compris les entités avec lesquelles il entretient des relations régulières sans toutefois exercer sur elles un contrôle de fait ou de droit (comme les sociétés d'économie mixte dans lesquelles elle détient une participation minoritaire).

468. Elles visent à permettre de décider d'entrer en relation avec un tiers, de poursuivre une relation en cours, le cas échéant avec des mesures de vigilance renforcées, ou d'y mettre fin (12).

Définition des modalités d'évaluation des tiers

469. Le recensement exhaustif des tiers, à travers le cas échéant une base existante, est de nature à faciliter la réalisation et la gestion de leur évaluation.

470. 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.

471. L'acteur public doit recenser de manière exhaustive ses catégories de tiers. Cette approche a pour objet de déterminer *ex ante*, sur le fondement de la cartographie des risques, les groupes de tiers qui l'exposent aux risques d'atteintes à la probité.

472. 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 groupes de tiers jugés pas ou peu risqués pourront ne pas faire l'objet d'une évaluation ou faire l'objet d'une évaluation simplifiée tandis que les groupes les plus risqués nécessiteront une évaluation approfondie. L'analyse des groupes de tiers pour déterminer ceux qui pourront ne

faire l'objet d'aucune évaluation est particulièrement opportune pour les services publics accessibles à de très nombreux usagers.

473. Au sein de chaque groupe de tiers qui nécessite une évaluation, le 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.

474. L'évaluation de l'intégrité des tiers permet à l'acteur public 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 peuvent conduire l'acteur public à réaliser une évaluation plus poussée ou à l'évaluer en priorité.

Modalités d'évaluation de l'intégrité des tiers

475. 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 collaborateur ou le service en charge du dispositif anticorruption (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.

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

477. Les informations et documents utiles à l'évaluation des tiers sont déterminés par l'acteur public sur le fondement de sa cartographie des risques. Dans bien des cas, une partie des données listées infra à titre indicatif est déjà demandée dans le cadre des procédures administratives d'instruction en vigueur.

478. A titre indicatif, les évaluations peuvent inclure :

- la collecte d'informations au moyen de la consultation de listes internes à l'acteur public ;
- 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, rapports de contrôle ou d'inspection...);
- 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 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.

479. Les informations sont obtenues dans le respect des réglementations applicables, notamment celles relatives à la protection des données personnelles.

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

481. L'acteur public s'assure que le tiers dispose de l'expérience, des qualifications et des compétences nécessaires à la réalisation de sa mission. A ce titre, il peut demander au tiers de lui communiquer les références professionnelles qu'il 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. Pour ce qui concerne les tiers ayant la qualité de pouvoir adjudicateur, ces vérifications s'effectuent dans le respect du code de la commande publique.

482. La collecte de données personnelles relatives à l'intégrité du tiers, qui peuvent porter sur d'éventuelles poursuites ou condamnations pour atteintes à la probité, doit respecter les normes régissant la protection des données.

483. L'acteur public peut également s'assurer que le tiers a mis en œuvre un dispositif anticorruption. Le fait que le tiers ne communique pas sur la mise en place d'un tel dispositif lorsqu'il y est contraint par la loi et ne le documente pas peut être considéré comme un facteur de risque.

Appréciation du niveau du risque du tiers

484. L'acteur public 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.

485. Certaines relations comportent un risque aigu d'atteintes à la probité comme, par exemple, le cas d'un tiers ayant pour mission d'assister l'acteur public dans l'obtention de contrats. Il peut inciter le tiers à se livrer à des pratiques non conformes de façon à contourner son dispositif anticorruption.

486. 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. De la même manière, le niveau de dépendance économique de l'acteur public vis-à-vis du tiers ou du tiers vis-à-vis de l'acteur public peut constituer un risque.

487. L'acteur public vérifie que le coût de la prestation 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.

488. 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.

489. 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 qui lui sont demandés peut être considéré comme un facteur de risque lors de son évaluation.

Conclusions à tirer des évaluations

490. A la suite de l'évaluation du niveau de risque, il peut être 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 (13) ;
- de reporter la prise de décision (pour cause d'évaluations complémentaires, par exemple).

491. Les personnes à l'origine de la décision sont clairement identifiées au sein de l'acteur public.

492. L'absence de facteurs de risque à la suite d'une évaluation ne garantit pas que la relation avec le tiers soit absolument dénuée de risque. A l'inverse, l'identification de facteurs de risque n'interdit pas la relation, mais doit conduire l'acteur public à prendre les mesures de vigilance appropriées pendant la relation.

Mesures de vigilance et de prévention à déployer en cours de relation avec un tiers

493. Les mesures de prévention et de détection des atteintes à la probité devant être adaptées à l'environnement de chaque acteur public, il revient à ce dernier de définir les mesures qu'il juge cohérentes avec ses spécificités.

494. Dans ce cadre, l'acteur public peut utilement envisager l'une ou plusieurs des options suivantes :

- informer le tiers de l'existence de son dispositif anticorruption en communiquant, par exemple, le code de conduite ;
- former ou sensibiliser le tiers au risque ;
- renforcer la collégialité dans la prise de décision ;
- renforcer le contrôle interne (notamment la validation hiérarchique) ;
- exiger du tiers un engagement écrit de lutte contre les atteintes à la probité ou insérer une clause permettant à l'acteur public de mettre un terme à la relation conventionnelle en cas de manquement à la probité si la nature juridique de la relation avec le tiers le permet.

Suivi de la relation contractuelle avec le tiers

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

496. A cet égard, l'acteur public doit avoir une visibilité complète sur les paiements reçus de tiers ou effectués à leur profit afin de s'assurer que le prix de la prestation et les modalités de paiement sont conformes aux dispositions contractuelles.

Evaluation des tiers et commande publique

497. L'évaluation de l'intégrité des tiers par les acteurs publics appliquant le code de la commande publique doit être menée dans le respect des principes fondamentaux de la commande publique : liberté d'accès à la commande publique, égalité de traitement des candidats et transparence des procédures.

498. Cette évaluation intègre les vérifications prévues par le code de la commande publique ; l'acteur public vérifie en particulier l'existence d'éventuelles mesures d'exclusion des procédures de marchés publics dont l'opérateur économique, candidat à un marché, est susceptible de faire l'objet :

- exclusion pour les entreprises ayant fait l'objet d'une condamnation définitive pour un certain nombre d'infractions, dont la corruption ;
- exclusions laissées à l'appréciation de l'acheteur :
 - en cas de candidature créant une situation de conflit d'intérêts et lorsqu'il ne peut y être remédié par d'autres moyens ;
 - en cas de tentative d'influence sur la décision ;
 - en cas de tentative d'obtention d'informations confidentielles.

499. L'évaluation des opérateurs économiques permet, au regard du risque identifié, d'adapter la relation entre le pouvoir adjudicateur et le ou les tiers. Ainsi, dans le cas d'un tiers risqué ou d'un secteur identifié dans la cartographie des risques comme sensible, l'acteur public peut prendre des mesures de prévention comme par exemple :

- renforcer la collégialité dans la prise de décision ;
- former les agents chargés de la préparation ou du suivi du marché ;

- organiser, le cas échéant, le retrait des personnes susceptibles d'intervenir dans la passation du marché et qui se trouvent en situation de conflits d'intérêts ;
- renforcer le contrôle interne (notamment les cas de validation hiérarchique) ;
- maintenir une vigilance élevée tout au long de l'exécution d'un marché conclu avec un tiers évalué comme risqué.

500. Dans la mesure où les critères d'analyse des offres doivent avoir un lien avec l'objet du marché ou ses conditions d'exécution, l'introduction de critères relatifs à l'engagement anticorruption des entreprises candidates ne paraît envisageable que dans des cas résiduels. L'ajout de tels critères pourrait exposer le pouvoir adjudicateur à des reproches de favoritisme.

Renouvellement et mise à jour des évaluations des tiers

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

502. Les informations sur la situation du tiers qui n'impactent pas le niveau de risque de l'acteur public donnent lieu à une mise à jour des informations sur le tiers. En revanche, si ces informations portent sur 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, alors une nouvelle évaluation du tiers est conduite.

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

Conservations des informations sur les tiers

504. 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 (ou après la date d'une opération occasionnelle), sous réserve d'une législation plus exigeante.

B. – Détection

1. Dispositif d'alerte interne

Définition et objectifs

505. Le dispositif d'alerte interne est la procédure mise en œuvre par les acteurs publics afin de permettre à leurs personnels de porter à la connaissance d'un référent dédié, un comportement ou une situation potentiellement contraire au code de conduite ou susceptibles de constituer des atteintes à la probité, afin d'y mettre fin et de prendre les sanctions appropriées, le cas échéant (cf. annexe 1).

506. Les administrations de l'Etat (administrations centrales, services à compétence nationale, services déconcentrés), les communes de plus de 10 000 habitants, les départements et les régions, les collectivités mentionnées à l'article 72-3 de la Constitution ainsi que les établissements publics en relevant et les établissements publics de coopération intercommunale à fiscalité propre regroupant au moins une commune de plus de 10 000 habitants, les autorités publiques indépendantes d'au moins cinquante agents et les autorités administratives indépendantes ainsi que toute autre personne morale de droit public ou de droit privé d'au moins cinquante agents ou salariés (établissements publics, groupement d'intérêt public, etc.) ont l'obligation de mettre en place des procédures appropriées de recueil des signalements émis par les membres de leur personnel ou par des collaborateurs extérieurs et occasionnels (article 8 de la loi).

507. Ces procédures doivent notamment permettre le signalement de délits (article 6 de la même loi) et concernent donc les situations de commission d'une atteinte à la probité.

508. Les agents affectés dans une collectivité, un établissement public ou un organisme non soumis à l'obligation de mettre en place une procédure de recueil des signalements peuvent également réaliser le signalement d'un délit, en respectant la procédure prévue au I de l'article 8 de la loi. Ils peuvent ainsi s'adresser à leur supérieur hiérarchique direct ou indirect.

509. Le statut général des fonctionnaires et le code du travail prévoient un régime protecteur en faveur des auteurs de l'alerte, dès lors qu'ils ont respecté les prévisions de la loi pour effectuer leur signalement (domaines susceptibles de faire l'objet d'une alerte et procédure).

510. Les agents relevant du statut général des fonctionnaires peuvent également effectuer un signalement concernant une situation de conflit d'intérêts, soit auprès de leur autorité hiérarchique, soit auprès de leur référent déontologue, en bénéficiant du même régime protecteur. Des situations qui, sans être constitutives du délit de prise illégale d'intérêts, apparaissent néanmoins comme contraires aux obligations déontologiques des agents publics, car constitutives d'un conflit d'intérêts peuvent ainsi faire l'objet d'un signalement.

511. Au regard des dispositifs d'ores et déjà applicables et dans l'attente de la transposition de la directive (UE) 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 sur la protection des personnes qui signalent des violations du droit de l'Union, l'AFA recommande la mise en place d'un dispositif d'alerte unique, non spécifique à l'anticorruption.

512. Toutefois, lorsqu'un signalement révèle une potentielle atteinte à la probité, une enquête interne doit être diligentée.

Articulation des différents dispositifs d'alerte

513. Différents dispositifs d'alerte professionnelle coexistent, il est conseillé, dans un souci de lisibilité, lorsque c'est juridiquement possible, la mise en place d'un dispositif technique unique de recueil des signalements, qui feront l'objet de traitement approprié.

514. 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 (14), ou aux ordres professionnels. Il peut également être rendu public.

Organisation du dispositif d'alerte

515. Le dispositif d'alerte interne doit être adapté au profil de risque de l'acteur public.

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

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

518. L'acteur public 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 ; il veille également à la formation des supérieurs hiérarchiques.

519. Le dispositif d'alerte interne est présenté sans délai aux collaborateurs venant de rejoindre l'acteur public.

520. 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 des moyens permettant d'en garantir la confidentialité. Les prestations fournies dans ce cadre devront faire l'objet de contrôles réguliers. L'acteur public 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'acteur public.

521. Le dispositif d'alerte interne est à déployer sur l'ensemble du périmètre de l'acteur public. Il est à adapter aux spécificités des entités qui le composent (activité, taille, législation locale...).

Traitement des alertes

522. 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.

523. Le dispositif d'alerte interne indique :

- le référent fonctionnellement désigné pour recueillir les alertes au sein de l'acteur public 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.

524. 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.

525. Dans l'hypothèse d'une mise en cause d'une ou plusieurs personnes, l'acteur public doit être vigilant lors de la réunion de preuves ou documents, notamment lorsque les personnes mises en cause dans l'alerte sont susceptibles de se concerter ou de détruire des données ou documents les incriminant.

526. 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 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 remis à l'appui de son signalement ;
- en cas d'enquête interne, les informations et documents professionnels transmis par l'auteur de l'alerte et 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 l'auteur du signalement et, le cas échéant, les personnes visées par celui-ci, de la clôture de la procédure.

527. 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.

528. 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.

529. 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)

530. 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 pourra prévoir notamment :

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

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

532. En cas d'externalisation de l'enquête interne, la conformité des services fournis 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.

533. Toute enquête interne est diligentée par une ou plusieurs personnes qualifiées, désignées par l'instance dirigeante de l'acteur public.

534. L'instance dirigeante est systématiquement informée des enquêtes ouvertes relatives aux situations les plus sensibles, à l'exception de celles où elle est visée.

535. A la suite d'une enquête interne, la rédaction formelle d'un rapport d'enquête est destinée à consigner l'ensemble des faits et preuves recueillis, 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.

536. Lorsque les soupçons apparaissent suffisamment étayés, ce rapport est communiqué à l'instance dirigeante (ou à l'organe de contrôle lorsqu'elle est visée) qui décide des suites à y donner.

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

538. Enfin, une action judiciaire peut être diligentée à l'encontre de la personne physique concernée si l'acteur public 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 tenue de le faire si elle relève des autorités énumérées à l'article 40 du code de procédure pénale.

539. 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 anticorruption (plan de formation, code de conduite, évaluation de l'intégrité des tiers).

Mise en œuvre du dispositif d'alerte interne

540. Les étapes suivantes peuvent utilement être observées :

- établissement d'une procédure formalisée qui peut notamment prévoir la désignation d'un référent alerte et la mise en place d'un comité intégrant des personnes qualifiées, soumises à des obligations de confidentialité. 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'acteur public peut décider d'ouvrir son dispositif d'alerte aux tiers. Il 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 niveaux sur la procédure d'alerte interne et intégration du dispositif d'alerte 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 ;
- mise en place d'indicateurs 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, etc.). Ces indicateurs sont transmis à l'instance dirigeante.

Archivage des alertes et de leur traitement

541. 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'effet.

542. Si le responsable du traitement décide de donner suite (15) à une alerte, ou qu'une action disciplinaire ou judiciaire est engagée, l'ensemble des données à caractère personnel collectées à l'occasion de l'instruction peut

être conservé jusqu'au terme de la procédure, jusqu'à acquisition de la prescription (six ans) ou épuisement des voies de recours.

543. Dans le cas où l'instruction de l'alerte ne débouche sur aucune suite, les données à caractère personnel doivent être supprimées dans les deux mois suivant la clôture de l'instruction.

544. Pour les alertes recueillies par le biais d'un dispositif technique unique de recueil, et ne concernant pas des faits susceptibles d'être qualifiés d'atteintes à la probité, 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'Etat.

545. La procédure d'alerte interne (articles 8 ou 17 de la loi) est distincte du signalement au procureur de la République prévu par l'article 40 du code de procédure pénale (16).

546. Plusieurs conditions sont exigées pour recourir à ce mode de signalement externe prévu à l'article 40 :

- les faits doivent être constitutifs d'un crime ou d'un délit ;
- ils doivent être « suffisamment établis » ;
- l'agent doit en avoir connaissance dans l'exercice de ses fonctions.

2. Le contrôle interne des risques d'atteintes à la probité

La contribution du dispositif de contrôle interne et d'audit interne à la prévention et à la détection des atteintes à la probité

547. Au sein des acteurs publics qui sont déjà dotés d'un dispositif de contrôle interne et d'audit interne non spécifique aux risques d'atteintes à la probité, celui-ci peut comprendre jusqu'à trois niveaux :

- les contrôles de premier niveau (17) visent à s'assurer que les tâches inhérentes à un processus opérationnel ou support ont été effectuées conformément aux procédures et aux finalités édictées par l'acteur public. Ils peuvent être opérés par les équipes opérationnelles ou support ou par leurs responsables hiérarchiques ;
- les contrôles de deuxième niveau (18) visent à s'assurer, selon une fréquence prédéfinie ou de façon aléatoire, de la bonne exécution des contrôles de premier niveau sur les processus opérationnels ou support. Ils sont réalisés par un service distinct de ceux qui gèrent et font fonctionner au quotidien chaque processus opérationnel ou support, comme les services en charge de la maîtrise des risques, du contrôle qualité, du contrôle de gestion, de la conformité, etc.

Les contrôles de premier et de deuxième niveaux, constitutifs du contrôle interne, sont formalisés au sein d'une procédure qui précise notamment les processus et situations à risque 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 de troisième niveau, également appelés « audits internes », visent à s'assurer que le dispositif de contrôle interne est conforme aux exigences de l'acteur public, efficacement mis en œuvre et tenu à jour.

548. Le dispositif visant à maîtriser les risques d'atteintes à la probité fait partie du dispositif de contrôle interne de l'acteur public. Il s'appuie sur les dispositifs de maîtrise des risques préexistants (risques financiers et risques opérationnels, en particulier) qui permettent d'ores et déjà de prévenir, détecter et maîtriser certains risques d'atteintes à la probité. L'AFA recommande aux acteurs publics de compléter, sur la base de la cartographie des risques d'atteintes à la probité, les procédures de contrôle interne afin qu'elles prennent en compte de manière pertinente ces risques.

549. La cartographie des risques d'atteintes à la probité, le plan d'actions, le plan de contrôle et le plan d'audit associés enrichissent ainsi le dispositif de contrôle interne et d'audit interne non spécifique aux risques d'atteintes à la probité de l'acteur public.

550. Le contrôle interne comptable, qui préexiste bien souvent au dispositif spécifique de maîtrise des risques d'atteintes à la probité, joue un rôle particulier dans la prévention et la détection des atteintes à la probité. Il convient donc, dans cette perspective, de veiller à son correct déploiement.

Les contrôles comptables

551. La fiabilité des comptes publics est un principe fondateur des finances publiques (19). De même, le principe de séparation des ordonnateurs et des comptables constitue une caractéristique propre aux acteurs publics, en application duquel l'ordonnateur prescrit les opérations financières tandis que le comptable exécute, après contrôle de régularité, l'opération comptable. Lui seul manie les fonds. Il assure par ailleurs un contrôle sur les régies. Cette incompatibilité des fonctions d'ordonnateur avec celles de comptable public vise à assurer une bonne gestion des deniers publics et à garantir la probité, les contrôles du comptable public étant destinés à repérer les erreurs ou irrégularités avant paiement. Les comptables publics ont un rôle de premier plan à jouer dans la détection des atteintes à la probité. Ce risque doit être pris en compte dans la détermination de la méthodologie du contrôle hiérarchisé de la dépense et du contrôle allégé en partenariat.

552. Parmi les procédures de contrôle et d'audit internes, les procédures de contrôle interne et d'audit comptable de l'ordonnateur, qui participent à la maîtrise des risques des organisations, constituent un instrument privilégié de prévention et de détection des atteintes à la probité. Le déploiement de systèmes d'information financière fiables et faciles à manier constitue un facteur clé de leur efficacité.

553. Le contrôle interne comptable permet de donner ainsi une assurance raisonnable sur la qualité des comptes, c'est-à-dire, leur fidélité à la réalité économique, patrimoniale et financière. Le contrôle interne intègre un audit

interne comptable et financier, à la charge d'un service distinct, permettant d'évaluer périodiquement l'efficacité du dispositif de contrôle interne.

554. Le recours éventuel à la certification des comptes par un tiers indépendant (comme les juridictions financières) ne dispense pas les acteurs publics concernés de concevoir et de mener les contrôles internes visant à s'assurer de la fiabilité des informations financières et à maîtriser leurs risques.

Définition et objectifs

555. Les contrôles comptables, ci-après « contrôles comptables anticorruption », ont pour objectif de s'assurer que les comptes ne sont pas utilisés pour masquer des faits d'atteintes à la probité.

Articulation avec les contrôles comptables en place

556. Les acteurs publics disposent de 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.

557. 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) ;
- 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.

558. 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 d'atteintes à la probité de l'acteur public.

559. Peuvent, par exemple, représenter des situations à risque et ainsi être traités les frais de représentation et de déplacement, le traitement des appels de fonds, la gestion des actifs immobiliers et des stocks, le fonctionnement des régies, les produits des services et du domaine, les éventuels engagements hors bilan.

Formalisation des contrôles comptables anticorruption

560. 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

561. 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).

562. 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.

563. 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.

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

565. 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.

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

567. 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.

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

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

570. Dans ce cadre, les audits comptables 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 d'atteintes à la probité) et de l'application des contrôles comptables anticorruption de premier niveau et de deuxième niveaux.

Traitement des anomalies constatées

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

572. Les cas d'anomalies alimentent également une mise à jour de la cartographie des risques d'atteintes à la probité et peuvent faire l'objet d'illustrations complémentaires dans le code de conduite et les supports de formation dédiés à leur prévention.

573. Si l'anomalie relève d'un manquement dans la mise en œuvre des procédures ou du dispositif de prévention et de détection des atteintes à la probité, 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.

574. Si l'anomalie fait ressortir des soupçons ou des faits d'atteintes à la probité, elle doit être portée à la connaissance de l'instance dirigeante qui peut décider de diligenter une enquête administrative.

C. – Contrôle et évaluation interne du dispositif anticorruption

1. Objectifs et modalités

575. Afin de s'assurer de l'adéquation et de l'efficacité des procédures de prévention et détection des atteintes à la probité, l'acteur public les contrôle et les évalue.

576. Ce dispositif répond à quatre objectifs :

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

577. Pour chacun des contrôles doivent être précisés :

- l'objet et le périmètre des contrôles ;
- 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, la fréquence du contrôle, la formalisation attendue ;
- la communication des résultats du contrôle et des mesures correctives pouvant être mises en place ;
- les modalités de conservation des pièces afférentes aux contrôles.

578. 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 anticorruption est conforme aux exigences de l'acteur public, 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 d'atteintes à la probité sont couvertes par des mesures de prévention efficaces.

2. Typologie de contrôles à déployer

579. Pour chaque mesure et procédure constitutive du dispositif anticorruption, des contrôles sont mis en œuvre.

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

Procédure	Points d'attention
Cartographie des risques d'atteintes à la probité	<ul style="list-style-type: none"> - s'assurer régulièrement de la pertinence du périmètre de la cartographie, de la méthodologie mise en œuvre, du déploiement des plans d'actions afférents ; - analyser les insuffisances constatées et notamment les incidents survenus afin de mettre à jour la cartographie.
Code de conduite et politiques/procédures annexées	<ul style="list-style-type: none"> - s'assurer de la mise en œuvre effective des procédures (par exemple, en matière d'acceptation de cadeaux et invitations), par des contrôles <i>a priori</i> et des contrôles <i>a posteriori</i> sur échantillons ; - s'assurer de la diffusion du code de conduite et de sa connaissance par les personnes concernées ; - s'assurer de manière régulière de la pertinence du code de conduite et des exemples de situations et comportements décrits dans le code (notamment si des incidents ont été constatés et en cas d'actualisation de la cartographie des risques).
Formation	<ul style="list-style-type: none"> - s'assurer que les formations prévues ont bien été réalisées et suivies par les personnes concernées (notamment les personnes particulièrement exposées et les personnes chargées de mettre en œuvre les procédures de lutte contre les atteintes à la probité) ; - s'assurer 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.

Procédure	Points d'attention
Évaluation des tiers	- s'assurer de la mise en œuvre effective des mesures de vigilance par des contrôles <i>a priori</i> et des contrôles <i>a posteriori</i> sur échantillons ; - vérifier régulièrement l'adéquation du dispositif d'évaluation des tiers au regard des risques identifiés dans la cartographie.
Alerte interne	- contrôler le déploiement et la correcte application de la procédure d'alerte ; - réaliser une 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 ? ...) ; - contrôler la pertinence des réponses apportées aux signalements reçus ; - contrôler les modalités d'archivage des signalements.
Contrôle interne et contrôles comptables	- s'assurer de la formalisation des procédures de contrôle ; - contrôler la mise en œuvre effective des contrôles prévus et leur traçabilité ; - vérifier régulièrement l'adéquation du dispositif de contrôle interne au regard des risques identifiés dans la cartographie.
Régime disciplinaire	- s'assurer que tout manquement au code de conduite et toute atteinte à la probité fait l'objet d'une sanction adaptée.

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

582. 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.

583. 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

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

D. – Remédiation

1. Gestion et suivi des insuffisances constatées

585. 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.

2. Régime disciplinaire

Définition

586. Le régime disciplinaire correspond aux sanctions qu'un acteur public est susceptible de prendre à l'encontre d'un collaborateur dont le comportement est fautif.

587. Sont notamment considérés comme une faute de nature à justifier une sanction disciplinaire, des comportements constitutifs d'une atteinte à la probité, un manquement au code de conduite (20) ou un manquement au devoir de probité.

Principe de gradation des sanctions

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

Mécanisme

589. L'engagement de l'instance dirigeante dans la maîtrise des risques d'atteintes à la probité implique, en cas de comportements constitutifs d'une atteinte à la probité, d'un manquement au code de conduite (21) ou d'un manquement au devoir de probité, d'engager une procédure disciplinaire et de mettre en œuvre des sanctions disciplinaires proportionnées.

590. Selon les cas, un dépôt de plainte ou un signalement au procureur de la République sur le fondement de l'article 40 du code de procédure pénale peuvent être réalisés parallèlement au lancement de la procédure disciplinaire.

591. L'instance dirigeante n'est pas tenue d'attendre la 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.

592. Dans le cas du code de conduite applicable aux élus, il appartient à l'instance dirigeante de tirer les conséquences du non-respect par l'un d'eux des dispositions de ce code. Cela peut, le cas échéant, conduire à, d'une part, modifier le périmètre de la délégation confiée à l' élu en question, voire à la lui retirer, d'autre part, à l'exclure de certaines instances comme la commission d'appel d'offres.

Mise en place d'un registre des sanctions

593. 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.

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

Communication interne

595. 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.

-
- (1) Sous réserve du respect des dispositions encadrant le processus considéré pour les acteurs publics.
- (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.
- (3) Collaborateur extérieur ou occasionnel (personnel intérimaire, stagiaire, prestataire de service, salarié des entreprises sous-traitantes, etc.)
- (4) « L'expression "suites" désigne toute décision prise par l'organisme pour tirer des conséquences de l'alerte. Il peut s'agir 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.
- (5) Il s'agit de contrôles préventifs réalisés avant que la décision ou l'opération ne soient mises en œuvre.
- (6) Il s'agit de contrôles détectifs conduits sur tout ou partie des décisions prises ou des opérations réalisées.
- (7) Articles 3 et 8 de la loi et décret n° 2017-564 du 20 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'Etat.
- (8) Notamment la loi n° 2013-907 du 11 octobre 2013 relative à la transparence de la vie publique ; la loi n° 83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires, modifiée par la loi n° 2016-483 du 20 avril 2016 relative à la déontologie et aux droits et obligations des fonctionnaires et par la loi n° 2019-828 du 6 août 2019 de transformation de la fonction publique, le décret n° 2020-69 du 30 janvier 2020 relatif aux contrôles déontologiques dans la fonction publique.
- (9) 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.
- (10) Un scénario de risque correspond à une situation susceptible de donner lieu à la commission d'une atteinte à la probité. Par exemple, la non déclaration d'un conflit d'intérêts par l'agent chargé de l'instruction d'une décision d'octroi de subvention concernant une association dont son conjoint est le président ou encore la non-réalisation de vérifications sur place de la part de l'agent chargé de certifier le service fait à réception de livraisons de la part d'un fournisseur.
- (11) S'agissant des services dont les personnels relèvent du statut général des fonctionnaires, le chef de service fait alors application de la compétence qui lui est reconnue par l'article 25 de la loi n° 83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires : « Tout chef de service peut préciser, après avis des représentants du personnel, les principes déontologiques applicables aux agents placés sous son autorité, en les adaptant aux missions du service ».
- (12) Sous réserve du respect des dispositions encadrant le processus considéré.
- (13) Cf. Note 12.
- (14) Collaborateur extérieur ou occasionnel (personnel intérimaire, stagiaire, prestataire de service, salarié des organisations sous-traitantes, etc.)
- (15) Cf. Note 4.
- (16) L'article 40 du code de procédure pénale : « Toute autorité constituée, tout officier public ou fonctionnaire qui, dans l'exercice de ses fonctions, acquiert la connaissance d'un crime ou d'un délit est tenu d'en donner avis sans délai au procureur de la République et de transmettre à ce magistrat tous les renseignements, procès-verbaux et actes qui y sont relatifs. »
- (17) Cf. Note 5.
- (18) Cf. Note 6.
- (19) L'article 47-2 de la Constitution consacre les principes de sincérité, de régularité et d'image fidèle pour toutes les administrations publiques.
- (20) Sous réserve, pour les personnels relevant du statut général des fonctionnaires, des précisions apportées au § 433 *supra*.
- (21) Cf. Note 20.

ANNEXES

ANNEXE N° 1

LE LANCEUR D'ALERTE (22)

596. 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.

597. 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 peut les porter à la connaissance de son supérieur hiérarchique, direct ou indirect, ou d'un référent désigné par l'employeur.

598. 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.

599. Le lanceur d'alerte peut également l'adresser au Défenseur des droits afin d'être orienté vers l'organisme approprié pour le recueil de l'alerte.

600. 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.

601. 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.

(22) <https://defenseurdesdroits.fr/>.

ANNEXE N° 2

EXEMPLE DE SCÉNARIOS DE RISQUES POUR LES ACTEURS PUBLICS

L'AFA a identifié des exemples de scénarios de risques dans les trois processus suivants de gestion publique :

- le versement de subventions ;
- la gestion des ressources humaines ;
- la commande publique.

En miroir, elle a également identifié des exemples de mesures de prévention et de détection, ainsi que de bonnes pratiques, de nature à atténuer les risques. Comme le précise le paragraphe 410 des présentes recommandations, l'AFA suggère aux acteurs publics, et notamment à ceux qui ne seraient pas familiarisés avec la démarche de cartographie des risques, d'examiner prioritairement ces processus de gestion publique au démarrage de leurs travaux de cartographie.

Ces exemples ne sont pas exhaustifs et sont à adapter et à compléter en fonction du profil de risque de chaque acteur public.

Nota. – Cette annexe fait partie intégrante des recommandations destinées aux acteurs publics qu'elle vient préciser et illustrer.

1. Versement de subventions

1.1. Principaux risques d'atteintes à la probité liés à l'attribution de subventions

L'attribution de subventions est particulièrement exposée aux risques de **détournement de fonds publics** et de **prise illégale d'intérêts** :

Détournement de fonds publics :

- En cas d'attribution d'une subvention à un organisme « écran ».
- Lorsque la subvention est versée malgré un dossier de demande incomplet.
- Lorsque les fonds publics sont versés non pas à l'organisme demandeur, mais à un tiers qui a substitué son identité bancaire à celle de l'association.
- Lorsque l'association affecte tout ou partie des fonds publics reçus à un usage autre que celui qui a justifié le versement de la subvention.

Prise illégale d'intérêts :

- Lorsque l'instruction du dossier est réalisée par un agent public qui a un intérêt à ce que la subvention soit ou non attribuée (par exemple, lorsque son conjoint est membre du bureau de l'association).
- Lorsque la personne qui décide de l'attribution de la subvention ou qui participe à une décision collective d'attribution dispose d'un intérêt à ce que la subvention soit ou ne soit pas attribuée.

1.2. Exemples de mesures de prévention et de détection des atteintes à la probité dans le cadre du processus de versement de subventions

- Former les agents publics et les élus à la gestion des conflits d'intérêts et aux solutions à mettre en œuvre : déport, abstention de toute instruction...
- Concevoir le dossier de demande de subvention de telle sorte qu'il permette de vérifier l'existence de l'organisme demandeur, la réalité de son activité et l'identité des personnes participant à sa direction.
- Réaliser une étude de notoriété de l'organisme demandeur.
- Mettre en place un contrôle de cohérence systématique entre l'identité de l'organisme attributaire de la subvention et l'identité du titulaire du compte bancaire sur lequel les fonds seront versés.
- Ne pas verser immédiatement l'intégralité de la subvention accordée et soumettre le ou les versement(s) ultérieur(s) à un compte rendu intermédiaire de gestion ; pratiquer des contrôles sur place.
- Prévoir une obligation de compte rendu de l'usage de la subvention attribuée.
- Mettre en place un contrôle, éventuellement par sondage, de l'instruction des dossiers de demande de subvention.

2. Gestion des ressources humaines

2.1. Principaux risques d'atteintes à la probité liés à la gestion des ressources humaines

Dans ses actes liés au recrutement, à la gestion de carrière et à la paie, la gestion des ressources humaines est particulièrement exposée aux risques de **corruption**, de **trafic d'influence**, de **prise illégale d'intérêts**, de **détournement de fonds publics** et de **concussion** :

Corruption et trafic d'influence :

- Lorsqu'un recrutement est décidé en contrepartie d'un avantage octroyé au recruteur ou à une personne qui exerce une influence sur le recruteur.

Prise illégale d'intérêts :

- Lorsqu'un recruteur ou un membre de jury ne déclare pas qu'il a des liens personnels avec un candidat et participe au processus de décision concernant son embauche ou sa promotion.

Détournement de fonds publics :

- Lorsqu'un recrutement est réalisé et que la personne embauchée et rémunérée ne travaille pas pour l'entité publique (emploi fictif).
- Lorsqu'un gestionnaire de carrière ou de paie crée un collaborateur fictif dans le système d'information de gestion des ressources humaines, lui associe son propre compte bancaire et perçoit, par ce biais, une rémunération liée à un emploi fictif.

Concussion :

- Lorsqu'un agent déclare des heures supplémentaires qu'il n'a pas effectuées pour toucher la rémunération associée.
- Lorsqu'un agent perçoit un traitement indiciaire indu après avoir volontairement fourni des éléments inexacts ayant conduit à une reconstitution de carrière à son avantage.

2.2. Exemples de mesures de prévention et de détection des atteintes à la probité dans le cadre du processus de subventionnement

- Former les agents à la gestion des conflits d'intérêts dans le cadre des recrutements et organiser un large accès au déontologue pour obtenir des conseils en la matière.
- Rapprocher régulièrement les fiches de paie avec l'organigramme nominatif du service.
- Automatiser autant que possible le calcul des avancements et reclassements dans le système d'information de gestion des ressources humaines et prévoir un contrôle hiérarchique en cas de forçage manuel.
- Empêcher l'habilitation informatique d'un agent pour intervenir sur son propre dossier dans le système d'information de gestion des ressources humaines.
- Vérifier systématiquement les évolutions atypiques des montants de la paie pour un même agent.
- Organiser des contrôles par sondage des saisies, par les pairs et par la chaîne hiérarchique.
- Organiser une rotation régulière des agents occupant des postes particulièrement exposés aux atteintes à la probité.

3. Commande publique

3.1. Principaux risques d'atteintes à la probité dans la commande publique

L'attribution des marchés publics est particulièrement exposée aux risques de **corruption** et de **trafic d'influence** :

- Attribution d'un marché à un acteur public en contrepartie d'une somme qu'il verse au décideur (corruption) ou qu'on lui propose de verser pour influencer un décideur public (trafic d'influence).

De plus, le non-respect des principes de la commande publique constitue en lui-même une atteinte à la probité, le **favoritisme** ; ces principes sont la liberté d'accès et l'égal accès des acteurs publics à la commande publique et la transparence des procédures. De nombreux types de situations recouvrent le risque de favoritisme :

- Choix inadapté de la procédure de consultation.
- Recours non justifié aux procédures dérogatoires (urgence/marché négocié sans mise en concurrence).
- Traitement plus favorable d'une des organisations au cours de la consultation (communication d'informations privilégiées, par exemple).
- Choix de critères d'analyse des offres biaisé ou « orienté ».
- Recours abusifs aux avenants.

Par ailleurs, la décision d'attribution d'un marché public peut conduire à une **prise illégale d'intérêts** dès lors que le décideur ou que l'un des décideurs dispose d'un intérêt quelconque dans la société candidate ou attributaire d'un marché :

- Participation d'un élu à la commission d'appel d'offres alors qu'une des organisations candidates est détenue par un membre de sa famille, même si elle n'est pas retenue.

Enfin, un risque de **détournement de fonds publics** est associé à l'exécution d'un marché public :

- Paiement de prestations ou de travaux commandés, mais non réalisés.
- Établissement d'un avenant dans des conditions contraires aux règles de la commande publique.
- Paiement de l'ensemble des prestations ou travaux commandés alors que la réalisation était partielle.

3.2 Exemples de mesures de prévention et de détection des atteintes à la probité dans les étapes de la commande publique

- Choix de la consultation : respect des règles que l'entité se fixe en matière de marchés à procédures adaptées (seuils), stricte application des critères justifiant le recours aux procédures dérogatoires.
- Consultation : donner le même niveau d'information à tous les candidats, justifier le choix des critères d'analyse des offres, notamment les critères techniques.
- Attribution : mettre en œuvre un déport des décideurs ayant un intérêt (financier ou moral), privilégier un choix collégial pour l'attribution des marchés à procédures adaptées.
- Exécution : porter une attention particulière au service fait, réaliser des contrôles réguliers sur les prestations ou travaux réellement réceptionnés (volume, qualité).