RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

AFA
Agence Française Anticorruption

PROJET DE MISE A JOUR DES RECOMMANDATIONS SUR LE REFERENTIEL ANTICORRUPTION APPLICABLE AUX ACTEURS PUBLICS (ARTICLE 3 DE LA LOI n°2016-1691 DU 9 DECEMBRE 2016)
– CONSULTATION NATIONALE -
Version du 15 OCTOBRE 2020

I. Introduction

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

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

3. Les présentes recommandations visent à faciliter la mise en place 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, (ci-après dénommées « acteurs publics» ou « organisations »), des mesures et procédures destinées à prévenir et détecter les faits d'atteintes à la probité. Elles déclinent pour ces organisations les recommandations générales définies par le référentiel commun (Cf. document distinct sur le référentiel commun).

I.1) Portée juridique des recommandations

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

5. D'autres méthodologies peuvent être employées sous réserve que leur mise en œuvre permette d'assurer la pertinence, la qualité et l'efficacité du dispositif de lutte contre les atteintes à la probité.

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

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

7. 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 appliquent les présentes recommandations en fonction de leur profil de risques.

8. Les organisations qui exercent un contrôle de droit ou de fait sur d'autres entités (par exemple : fondations, filiales, sociétés d'économie mixte (SEM), services publics locaux (SPL), établissements publics et autres entités satellites) s'assurent de la qualité et de l'efficacité du dispositif de prévention et de détection des atteintes à la probité déployé dans l'ensemble du périmètre qu'elles contrôlent.

9. L'AFA recommande également de veiller à ce que le dispositif anticorruption de l'organisation intègre, outre ses agents et collaborateurs, l'ensemble des membres des instances dirigeantes et les membres de leurs cabinets ainsi que, si nécessaire, les bénévoles contribuant à ses activités.

II. La mise en œuvre du référentiel anticorruption

10. La loi n° 2016-1691 du 9 décembre 2016, (ci-après « la loi »), dispose en son article 3, que l'AFA contrôle, de sa propre initiative, la qualité et l'efficacité des procédures mises en œuvre par les acteurs publics 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.

11. Les présentes recommandations visent à aider les acteurs publics à définir et à mettre en œuvre des mesures et procédures de prévention et de détection pertinentes et efficaces.

12. Les acteurs publics sont invités à mettre en œuvre la méthodologie préconisée par l'AFA dans ses recommandations. Ils peuvent tout autant recourir à d'autres approches méthodologiques de qualité équivalente et permettant d'atteindre les mêmes résultats.

13. Les présentes recommandations déclinent pour les acteurs publics le référentiel anticorruption commun qui repose sur trois piliers indissociables : l'engagement de l'instance dirigeante, la connaissance des risques d'atteinte à la probité à travers l'établissement d'une cartographie des risques et la gestion de ces risques par la mise en œuvre de mesures de prévention, de détection et de remédiation.

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

14. Les obligations qui s'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 du 9 décembre 2016[1] mais également, pour certains d'entre eux, de diverses dispositions législatives et réglementaires. Il s'agit notamment, pour les organisations 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.)[2.] 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 relatif à la gestion budgétaire et comptable publique.

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

16. 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. Les recommandations de l'AFA ont pour objectif d'aider les acteurs publics à élaborer un tel dispositif.

[1] 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.

[2] 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° 2017-105 du 27 janvier 2017 relatif à l'exercice d'activités privées par des agents publics et certains agents contractuels de droit privé ayant cessé leurs fonctions, aux cumuls d'activités et à la commission de déontologie de la fonction publique.

1. Définition et responsabilité de l'instance dirigeante

17. Constitue l'instance dirigeante les personnes - élues ou nommées - chargées d'administrer et de gérer une organisation, en application de ses statuts et des textes législatifs et réglementaires en vigueur.

18. Il s'agit, pour les entités publiques, des personnes ou instances suivantes :

- Pour les services de l'Etat : ministre, secrétaire général, directeur d'administration centrale, préfet de département ou de région, responsable de services déconcentrés.
- Pour le service public local : maire, président d'établissement public de coopération intercommunale (EPCI), de conseil départemental ou régional… Sont également inclus dans cette catégorie, les membres de l'assemblée délibérante (conseil municipal, communautaire, métropolitain, départemental, ou régional), mais également les directeurs généraux des services.
- Pour les établissements publics, sociétés d'économie mixte: président du conseil d'administration, conseil d'administration et directeur.
- Pour les établissements publics de santé : directeur, directoire, conseil de surveillance.
- 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 les membres des instances collégiales et le directeur ;
- Pour les associations reconnues d'utilité publique : président de l'assemblée générale, président du conseil d'administration, président du bureau ainsi que les membres des instances collégiales et le directeur.

19. 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 de prévention et de détection des atteintes à la probité.

2. Responsabilité de l'instance dirigeante

20. L'instance dirigeante veille à ce que les obligations existantes soient mises en perspective dans le cadre du dispositif de prévention et de détection des atteintes à la probité. Elle s'engage à mettre en œuvre une politique de tolérance zéro envers tout comportement qui pourrait y contrevenir, promeut et diffuse la culture de la probité au sein de l'organisation et vis-à-vis des tiers, en érigeant la prévention et la détection des atteintes à la probité à un niveau prioritaire.

21. La responsabilité de la mise en place du dispositif de prévention et de détection des atteintes à la probité 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.

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

23. L'instance dirigeante définit la stratégie de gestion des risques et s'assure de la mise en œuvre et de l'efficacité du dispositif de prévention et de détection des atteintes à la probité. A cet égard, elle veille à formaliser l'approbation de ce dispositif, et en particulier de la cartographie des risques. 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.

24. 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.

25. L'instance dirigeante vérifie, au moyen d'indicateurs et de rapports de contrôle et d'audit, que le dispositif de prévention et de détection est organisé, efficace et à jour.

26. La mise en œuvre des mesures et procédures qui composent le dispositif de prévention et de détection induit pour l'instance dirigeante d'intégrer des mesures de maîtrise des risques aux procédures et politiques publiques exposées de son organisation (cf. Annexe 1), notamment la gestion des ressources humaines, la commande publique et l'attribution de subventions publiques.

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

- les actes liés au recrutement, à la gestion de carrière et à la paie, ne peuvent donner lieu à des pratiques corruptives;
- 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.

28. En matière de commande publique, l'instance dirigeante s'assure que l'attribution des marchés publics, et plus largement le cycle complet de l'achat, se déroule non seulement dans le respect des principes généraux de la commande publique mais prévienne également tout risque d'atteinte à la probité qui pourrait entacher la procédure.

29. En matière de versement de subventions publiques, l'instance dirigeante s'assure que les procédures permettent d'éviter tout risque de détournement de fonds publics et de prise illégale d'intérêts.

30. L'instance dirigeante applique des sanctions adéquates du régime disciplinaire en cas d'atteinte à la probité.

31. L'instance dirigeante veille à ce que les « satellites » que contrôle l'organisation (en droit ou en fait) soient couverts par un dispositif de prévention et de détection des atteintes à la probité.

3. Moyens dédiés

32. La mise en œuvre d'un dispositif de prévention et de détection nécessite des moyens humains et financiers proportionnés au profil de risque de l'organisation.

33. 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'organisation ;
- les moyens matériels et humains affectés ou susceptibles d'être mobilisés.

34. 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.

35. Son positionnement dans l'organisation doit lui garantir:

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

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

4. **Une politique de communication interne et externe adaptée**

37. 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…), afin de dissuader les sollicitations indues des partenaires extérieurs.

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

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

40. Indispensable instrument de la connaissance des risques d'atteintes à la probité, la cartographie des risques permet aux organisations 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 leur réalisation.

41. Il est recommandé aux acteurs publics de mettre en place une cartographie des risques d'atteintes à la probité similaire à celle exigée des acteurs économiques soumis à l'article 17 de la loi précitée. Cette cartographie peut être spécifique ou intégrée dans une cartographie générale des risques, sous réserve de l'utilisation d'une méthodologie garantissant notamment 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.

42. 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 de la loi.

43. 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 de l'article 17), la cartographie doit intégrer les risques relatifs à l'ensemble des infractions d'atteintes à la probité exposées précédemment.

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

- de disposer d'une connaissance précise de l'organisation et de ses activités, dont les processus[3] managériaux, opérationnels et support que ces activités nécessitent de mettre en œuvre. Cette connaissance est la condition préalable à l'analyse fine des processus qui garantit que la cartographie des risques d'atteintes à la probité reflète fidèlement les risques auxquels l'organisation est réellement exposée. Chaque organisation établit sa propre cartographie des risques, qui lui est spécifique, et ne peut en conséquence être transposée en l'état à une autre organisation.
- 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

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

46. Elle donne à l'instance dirigeante la visibilité nécessaire pour la mise en œuvre de mesures de prévention et de détection efficaces, proportionnées aux enjeux identifiés par la cartographie et adaptées aux activités de l'organisation concernée.

47. Deuxième pilier du dispositif de prévention et de détection, la cartographie des risques d'atteintes à la probité permet à l'organisation de gérer efficacement ses risques à travers les mesures et procédures de prévention, de détection et de remédiation développées ci-dessous. Réciproquement, les enseignements

[3] 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.

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

48. 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 travaillant dans l'organisation, quel que soit leur statut (agents titulaires, agents contractuels, agents détachés ou mis à disposition, personnels sous contrat de droit privé, vacataires, apprentis, bénévoles).
- Ensuite, « de bout en bout », les processus managériaux, opérationnels et support mis en œuvre par l'organisation dans le cadre de ses activités. Elle appréhende les risques d'atteintes à la probité en prenant en compte les particularités de chaque organisation : missions, compétences, spécialité, structure de gouvernance et circuits de décision, statut des personnels, territoires, typologies de tiers, ressources propres, etc.
- Enfin, le périmètre d'intervention de l'organisation, soit l'ensemble des structures, notamment les satellites. Lorsque l'organisation dispose de la personnalité juridique, la responsabilité de faire établir une cartographie des risques d'atteintes à la probité incombe en premier lieu à ses dirigeants. Il appartient en second lieu à l'autorité de tutelle de s'assurer de l'existence de cette cartographie.

49. 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 de prévention et de détection des atteintes à la probité.

50. Au choix de l'organisation, 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.

51. 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'organisation. A la faveur de son actualisation, la cartographie participe d'un processus d'amélioration continue permettant aux organisations 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

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

53. 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.

54. 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'organisation a d'ores et déjà procédé à une description de tout ou partie de ses processus et elle 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.

1ère étape : Rôles et responsabilités des parties prenantes à la cartographie des risques d'atteintes à la probité

55. Au sein des organisations, les rôles et responsabilités sont répartis comme suit :

- l'instance dirigeante promeut l'exercice de cartographie des risques et donne les moyens de sa mise en œuvre au 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 l'organisation 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'organisation, apportent leur contribution à l'exercice de cartographie en rendant compte des facteurs spécifiques aux fonctions exercées et aux risques encourus.

56. L'organisation, lors de l'élaboration de sa cartographie, veille à appréhender les risques inhérents aux activités exercées par l'ensemble des personnels travaillant dans la structure, quel que soit leur statut, ainsi que ceux attachés aux missions des élus et de leurs collaborateurs.

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

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

58. Sur la base du recensement des processus, l'organisation organise des échanges avec des personnels de tout niveau hiérarchique et de toutes les fonctions de l'organisation choisis pour leur maîtrise de la mise en œuvre opérationnelle de ces processus. Ces échanges permettent la libre expression des participants et font l'objet de comptes rendus écrits.

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

60. La cartographie des risques intègre l'intervention des tiers de l'organisation, qui peut présenter un risque d'exposition à une sollicitation (facteur de risque). Afin de prévenir le risque de sollicitation externe, l'organisation met par ailleurs en œuvre des procédures d'évaluation des tiers adaptées au niveau de risque.

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

- le fonctionnement interne de l'organisation et notamment sa gouvernance ;
- ses activités : la fourniture de services, la réalisation de travaux, la délivrance d'autorisations, l'attribution de subventions, l'exercice des fonctions supports, la tenue de la comptabilité, la commande publique, les ressources humaines, la logistique ;
- 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 du tiers, secteur d'activité du tiers, relation directe ou indirecte, dépendance économique ;
- l'historique des incidents : doivent être pris en compte notamment les incidents ayant affecté l'organisation, révélés par les audits interne ou par les dispositifs d'alerte interne et déontologique, les faits ayant donné lieu à l'application du régime disciplinaire et à des décisions juridictionnelles concernant des organisations similaires, les observations de la Cour des comptes et de la chambre régionale des comptes, le retour d'expérience tiré du contrôle de légalité.

3ème étape : Evaluation des risques bruts

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

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

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

65. 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).

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

67. 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'organisation veille notamment à ce que les évaluations des risques bruts émanant de ses différentes composantes puissent être agrégées de manière cohérente.

4ème étape : Evaluation des risques nets ou résiduels

68. Cette étape vise à évaluer le niveau de maîtrise des risques par l'organisation 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.

69. 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.

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

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

71. Lorsque ces scénarios de risques présentent une évaluation nette de même niveau, il convient de les hiérarchiser au moyen d'une méthodologie objective adaptée aux activités spécifiques de l'organisation, reposant sur la combinaison de plusieurs critères comme la part du budget consacré, la nature et le type de relations avec les tiers.

72. 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.

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

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

74. 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. Elle peut être, au choix de l'organisation, organisée par compétence, par processus, par entité ou par territoire. 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 d'atteintes à la probité.

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

76. 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'organisation est exposée.

~~*77.*~~ Il est recommandé de conserver tous les éléments permettant d'apprécier la mise en œuvre effective des modalités et méthodologies de la cartographie.

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

II.3) Prévention des risques d'atteintes à la probité

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

- **Déontologie**

79. Dans une entité publique, le code de conduite rappelle et précise les conditions de mise en œuvre des obligations déontologiques applicables aux personnels et aux instances dirigeantes et notamment l'obligation :

- d'exercer ses fonctions avec intégrité et probité ;
- de prévenir et de faire cesser immédiatement tout conflit d'intérêts.

80. Pour les agents publics, ces obligations découlent du statut de la fonction publique (art. 25 à 26 de la loi n°83-634 du 13 juillet 1983) et, pour les instances dirigeantes publiques de la loi n°2013-907 du 11 octobre 2013 (art. 1er).

81. Peuvent être également rappelées dans le code de conduite les règles déontologiques applicables en matière de cumul d'activités, de mobilité vers le secteur privé et de retour vers le secteur public.

82. Si le code de conduite est un vecteur essentiel de la promotion des obligations déontologiques, d'autres outils ou procédures sont susceptibles de concourir à leur plein respect, comme le déploiement de formations facilitant l'identification et l'appréciation par les personnes concernées de leurs liens d'intérêts, la mise en place de procédures de recueil des liens d'intérêts des élus régulièrement mises à jour et utilisées dans la gestion des votes des assemblées, la mise en place de procédures de recueil et de contrôle des demandes et autorisations de cumuls d'activités.

- **Définition et objectifs du code de conduite**

83. Le code de conduite, quelle que soit la dénomination retenue par l'organisation, est un document qui manifeste la décision de l'instance dirigeante d'engager l'organisation 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.

84. Le code de conduite définit et illustre, à travers des exemples d'activités de l'organisation, les différents types de comportements à proscrire comme étant susceptibles de caractériser des atteintes à la probité.

- **Champ d'application**

85. Le code de conduite est applicable à l'ensemble des personnels de l'organisation, ainsi que, le cas échéant, aux élus et à leurs collaborateurs.

86. Concernant les autres collaborateurs de l'organisation (bénévoles, stagiaires), il est recommandé que le code leur soit communiqué et leur soit rendu opposable, dans le respect des dispositions légales applicables.

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

87. 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.

88. 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.

- **Contenu**

89. 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 de l'organisation, dans la mesure où il décrit les comportements à proscrire à partir des risques spécifiques à l'organisation.

90. Le code de conduite n'est pas limité à un recueil de bonnes pratiques, mais 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'organisation. A ce titre, il peut traiter notamment des cadeaux et invitations, des conflits d'intérêts et des frais de représentation. Une structuration en rubriques correspondant aux différents types de comportements à proscrire est encouragée.

91. Il est appuyé d'illustrations pertinentes au regard de l'activité de l'organisation et des risques définis dans sa cartographie des risques d'atteintes à la probité.

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

93. Le code de conduite prévoit que les comportements proscrits et, plus généralement, les comportements non conformes aux engagements et principes de l'organisation en matière de prévention et de détection des atteintes à la probité sont susceptibles de faire l'objet de sanctions disciplinaires dans le respect des dispositions disciplinaires applicables.

94. Le code de conduite mentionne le nom et les coordonnées des personnes qualifiées pour répondre aux questions soulevées par l'organisation (référent déontologue) et celles du référent alerte.

Formalisation et accessibilité du code de conduite »

95. 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.

96. Le code de conduite est communiqué en interne et constitue l'un des éléments auxquels sont formés les personnels de l'organisation.

97. 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'organisation concernée.

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

98. Le code de conduite rappelle et précise les modalités de mise en œuvre des obligations déontologiques applicables au personnel et aux dirigeants de l'organisation.

99. Certaines de ces obligations peuvent être d'origine législative ou réglementaire. Elles doivent alors être rappelées aux agents ou dirigeants concernés, et faire l'objet de précisions quant à leur mise en œuvre opérationnelle. En outre, ces obligations peuvent être utilement complétées par des mesures propres à l'organisation, en fonction de son profil de risque.

100. Le code de conduite peut ainsi détailler :

- les obligations d'intégrité et de probité de l'article 25 du statut de la fonction publique et citées dans l'article 1er de la loi 11 octobre 2013 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 dans l'organisation ;
- les dispositions relatives aux déclarations d'intérêts et de situation patrimoniale applicables dans l'organisation ;
- 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'organisation est concernée ;
- 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'organisation.

101. Le code de conduite peut renvoyer à des fiches « opérationnelles » (ou « processus », ou « procédures » relative 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 ces documents constituent un ensemble cohérent, clairement articulé et dont la lisibilité et l'accessibilité soit assurée pour tous les collaborateurs.

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

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

- **Mise à jour**

103. 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**

104. Vecteur de la culture d'intégrité au sein de l'organisation, 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 de l'organisation.

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

106. 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'organisation.

107. Le dispositif de sensibilisation et de formation doit :

- être coordonné avec les autres mesures et procédures du dispositif de prévention et de détection des atteintes à la probité. Ex : 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**

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

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

- l'engagement de l'instance dirigeante et le code de conduite ;
- les atteintes à la probité en général, leurs enjeux, leurs formes et les sanctions 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.

110. 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 dans l'organisation et son environnement.

- **Formation obligatoire destinée aux personnes les plus exposées**

111. La formation 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 risques.

112. Ces formations visent à ce que les personnes concernées s'approprient le dispositif de prévention et de détection des atteintes à la probité de l'organisation.

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

114. 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 de prévention et de détection (ou tout autre responsable désigné), les cadres et les personnels les plus exposés aux risques d'atteintes à la probité, c'est-à-dire les personnes en charge ou participant aux processus à risque.

115. Il peut s'agir, en particulier :

- 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 de prévention et de détection.

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

117. 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.

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

119. La formation implique une compréhension et une connaissance :

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

120. Le tronc commun de ces formations porte sur :

- l'engagement de l'instance dirigeante et 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 de prévention et de détection des atteintes à la probité ;
- 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.

121. 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.

122. Les personnels et cadre les plus exposés sont formés dès leur prise de fonction. Les formations sont régulièrement dispensées tout au long de l'exercice de leur fonction.

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

124. 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.

125. Des membres de l'organisation 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.

126. 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.

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

128. Dans l'hypothèse d'une externalisation, il est nécessaire que l'organisation 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…).

129. 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**

130. 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.

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

132. Dans l'hypothèse d'une externalisation des formations, le collaborateur ou le service responsable du dispositif de prévention et de détection des atteintes à la probité (ou tout autre responsable désigné) doit non seulement être informé du calendrier des formations et de leur contenu pédagogique, mais 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**

133. 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'organisation 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'organisation est en relation dans le cadre de ses missions, y compris les entités avec lesquelles l'organisation entretient des relations régulières sans toutefois exercer un contrôle de fait ou de droit (comme les sociétés d'économie mixte dans lesquelles elle détient une participation minoritaire).

134. Elles visent :

- d'une part, à permettre de décider d'entrer en relation avec un tiers[4], de poursuivre une relation en cours ou d'y mettre fin ;
- d'autre part, à optimiser l'efficacité des mesures de prévention et de détection des atteintes à la probité.

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

135. 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.

[4] Sous réserve de l'application des règles de la commande publique.

136. 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.

137. L'organisation 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 catégories de tiers qui l'exposent aux risques d'atteintes à la probité.

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

139. Au sein de chaque catégorie 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.

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

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

141. 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 de prévention et de détection des atteintes à la probité (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.

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

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

144. À titre indicatif, les évaluations peuvent inclure :

  - la collecte d'informations au moyen de la consultation de listes internes à l'organisation ;
  - 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.

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

146. L'organisation 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.

147. L'organisation s'assure que le tiers (en particulier s'il s'agit d'un fournisseur ou d'un prestataire) 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.

148. 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.

149. L'organisation 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 lorsqu'il y est contraint par la loi et ne le documente pas peut être considéré comme un facteur de risque.

- **Evaluation des tiers et commande publique**

150. L'évaluation de l'intégrité des tiers par les organisations 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.

151. Cette évaluation intègre les vérifications prévues par le code de la commande publique ; elle 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 de plein droit pour les entreprises ayant fait l'objet d'une condamnation définitive pour un certain nombre d'infractions, dont la corruption ;
- exclusions facultatives 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 de tentative d'obtention d'informations confidentielles.

152. 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'organisation 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 ;
- maintenir une vigilance élevée tout au long de l'exécution d'un marché conclu avec un tiers évalué comme risqué.

153. 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 pas envisageable. L'ajout de tels critères pourrait exposer le pouvoir adjudicateur à des reproches de favoritisme.

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

154. L'organisation 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.

155. 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'organisation dans l'obtention de contrats : d'une part, l'organisation peut inciter le tiers à se livrer à des pratiques non conformes de façon à contourner son dispositif de prévention et de détection des atteintes à la probité ; d'autre part, le tiers peut se livrer à de telles pratiques de sa propre initiative, sans que l'organisation n'en soit informée.

156. 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'organisation vis-à-vis du tiers ou du tiers vis-à-vis de l'organisation peut constituer un risque.

157. L'organisation 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.

158. 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.

159. 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**

160. À 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 ;
- de reporter la prise de décision (pour cause d'évaluations complémentaires, par exemple).

161. Les personnes à l'origine de la décision sont clairement identifiées dans l'organisation.

162. 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. À l'inverse, l'identification de facteurs de risques n'interdit pas la relation, mais doit conduire l'organisation 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**

163. Les mesures de prévention et de détection des atteintes à la probité devant être adaptées à l'environnement de chaque organisation, il revient à cette dernière de définir les mesures qu'elle juge cohérentes avec ses spécificités.

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

  - informer le tiers de l'existence de son dispositif de prévention et de détection des atteintes à la probité en communiquant, par exemple, le code de conduite ;
  - former ou sensibiliser le tiers au risque;
  - exiger du tiers un engagement écrit de lutte contre les atteintes à la probité ou insérer une clause permettant à l'organisation de mettre un terme à la relation contractuelle en cas de manquement à la probité si la nature juridique du contrat le permet;
  - exiger du tiers qu'il vérifie l'intégrité de ses sous-traitants afin de sécuriser la chaine contractuelle.

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

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

166. A cet égard, l'organisation doit avoir une visibilité complète sur les paiements reçus de tiers ou effectués aux tiers afin de s'assurer que la rémunération et les modalités de paiement sont conformes aux dispositions contractuelles.

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

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

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

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

170. 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**

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

II.4) Détection des atteintes à la probité

1. Dispositif d'alerte interne

- **Définition et objectifs**

172. Le dispositif d'alerte interne est la procédure mise en œuvre par les organisations 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, afin d'y mettre fin et de prendre les sanctions appropriées, le cas échéant.

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

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

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

175. 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.

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

177. En outre, la mise en place d'un seul et unique dispositif technique de recueil suppose d'ouvrir la possibilité de signalement non seulement aux personnels, mais aussi aux collaborateurs extérieurs et occasionnels[5].

178. 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.

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

180. 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.

181. Toutefois, si le signalement porte sur des atteintes au devoir de probité, il pourra être adressé directement à l'AFA. Le cas échéant, l'Agence le communiquera au procureur de la République compétent en application de l'article 40 du code de procédure pénale.

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

182. Enfin, à défaut de traitement dans un délai de trois mois par l'un des organismes saisis, le signalement pourra être rendu public.

183. 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 du 9 décembre 2016 peut être adressé directement à l'autorité judiciaire, à l'autorité administrative ou aux ordres professionnels. Il peut également être rendu public.

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

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

« *un lanceur d'alerte est une personne physique qui révèle ou signale, de manière désintéressée et de bonne foi, un crime ou un délit, une violation grave et manifeste d'un engagement international régulièrement ratifié ou approuvé par la France, d'un acte unilatéral d'une organisation internationale pris sur le fondement d'un tel engagement, de la loi ou du règlement, ou une menace ou un préjudice graves pour l'intérêt général, dont elle a eu personnellement connaissance.*

Les faits, informations ou documents, quel que soit leur forme ou leur support, couverts par le secret de la défense nationale, le secret médical ou le secret des relations entre un avocat et son client sont exclus du régime de l'alerte défini par le présent chapitre. »

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

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

  Sur ce point, l'auteur d'allégations qu'il sait fausses ne peut être considéré comme « *de bonne foi* » et encourt les poursuites prévues par la loi à l'encontre des auteurs de dénonciations calomnieuses (article 222-10 du code pénal).
- les faits révélés sont <u>graves</u> : ce critère s'apprécie au regard de la loi, qui mentionne un crime ou un délit, une violation grave et manifeste d'un engagement international pris par la France, ou d'un acte d'une organisation internationale pris sur ce fondement, ou une menace ou un préjudice graves pour l'intérêt général. Les délits d'atteintes à la probité répondent à ce critère de gravité.

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

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

- **Organisation du dispositif d'alerte**

187. Le dispositif d'alerte interne doit être adapté au profil de risque de l'organisation.

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

189. 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.

190. L'organisation 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.

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

192. 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'organisation 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'organisation.

- **Traitement des alertes**

193. La procédure d'alerte interne doit préciser les différentes étapes à suivre pour effecteur 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.

194. Le dispositif d'alerte interne indique:

- 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 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.

195. 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.

196. Dans l'hypothèse d'une mise en cause d'une ou plusieurs personnes, l'organisation doit être vigilante 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.

197. 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 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.

198. 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.

199. 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.

200. 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 boite postale)

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

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

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

203. 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.

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

205. L'instance dirigeante est systématiquement informée des enquêtes ouvertes. Elle intervient dans les situations les plus sensibles.

206. 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.

207. Lorsque les soupçons apparaissent suffisamment étayés, ce rapport est communiqué à l'instance dirigeante qui décide des suites à y donner.

208. 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.

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

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

- **Périmètre**

211. Le dispositif d'alerte interne est à déployer sur l'ensemble du périmètre de l'organisation. Il est à adapter aux spécificités des entités qui le compose (activité, taille, législation locale…).

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

212. Les étapes suivantes sont à réaliser :

  - Etablissement d'une procédure formalisée qui prévoit notamment la mise en place d'un comité intégrant des personnes qualifiées. Ce comité assure une prise de décision collégiale sur les suites à réserver aux alertes reçues.
  - Insertion d'un chapitre sur le dispositif d'alerte dans le code de conduite renvoyant à ladite procédure ;
  - Diffusion de la procédure d'alerte interne à l'ensemble des personnels par tous moyens (courrier de la direction, affichage, site intranet, remise en main propre,….) permettant de s'assurer que chaque personne concernée en a connaissance et y a accès. Dans le cas d'un dispositif d'alerte commun à l'alerte anticorruption et à d'autres dispositifs légaux, la procédure doit être également diffusée aux collaborateurs occasionnels. L'organisation peut décider d'ouvrir son dispositif d'alerte aux tiers. L'organisation peut choisir de mettre à profit ses outils de communication externes pour mentionner l'existence de son dispositif d'alerte (par exemple son site internet, les documents remis à ses tiers…) ;
  - Présentation du dispositif d'alerte dans le cadre des actions de sensibilisation de l'ensemble des personnels ;
  - Formation des personnels amenés à recueillir, gérer et traiter les alertes, notamment sur les obligations de confidentialité, et formation des personnels les plus exposés ;

- Mise en place des contrôles de premier et second niveau sur la procédure d'alerte interne et intégration du dispositif d'alerte dans le plan de contrôle de l'audit interne au titre du contrôle de troisième niveau. Pour éviter toute situation de conflit d'intérêts ou d'autocontrôle, les trois niveaux de contrôles rappelés ci-dessus peuvent être adaptés. Il importe, le cas échéant, que le personnel qui traite l'alerte soit différent de celui qui en contrôle le bon traitement et qu'un contrôle *a posteriori* soit effectué.

- **Indicateurs**

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

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

214. 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.

215. Si le responsable du traitement décide de donner suite[6] 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.

216. .

217. 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.

218. 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.

219. La procédure d'alerte interne (articles 8 ou 17 de la loi du 9 décembre 2016) est distincte du signalement au procureur de la République prévu par l'article 40 du code de procédure pénale[7].

220. 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.

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

[7] 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.* »

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**

221. Dans les organisations qui sont déjà dotées 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, (contrôles *a priori)*, 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'organisation. Ils peuvent être opérés par les équipes opérationnelles ou support ou par leurs responsables hiérarchiques ;
- Les contrôles de deuxième niveau (contrôle *a posteriori*) 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 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 de troisième niveau, également appelés « audits internes », visent à s'assurer que le dispositif de contrôle interne est conforme aux exigences de l'organisation, efficacement mis en œuvre et tenu à jour.

222. Le dispositif visant à maîtriser les risques d'atteintes à la probité converge partiellement avec le dispositif de contrôle interne et d'audit interne non spécifique aux risques de corruption. Ces deux dispositifs peuvent, en effet, avoir en commun certains scénarios de risque et certaines mesures de contrôle.

244. En effet, l'organisation est en mesure, sur le fondement de la cartographie des risques d'atteintes à la probité :

- d'identifier des situations à risque en matière d'atteintes à la probité,
- d'identifier et d'évaluer les dispositifs de contrôle de premier, deuxième et troisième niveaux non spécifiques aux risques d'atteintes à la probité concourant à maîtriser ces risques
- d'identifier les situations pas ou peu couvertes par ces mesures de contrôle, auxquelles il doit être remédié par un plan d'actions spécifique aux risques d'atteintes à la probité.

245. La cartographie des risques d'atteintes à la probité, le plan d'actions 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'organisation.

246. Parmi les dispositifs de maîtrise des risques non spécifiques aux risques d'atteintes à la probité, le contrôle interne comptable joue un rôle particulier dans la prévention et la détection des atteintes à la probité.

- **Les contrôles comptables**

247. La fiabilité des comptes publics est un principe fondateur des finances publiques[8]. 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 le 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.

248. Parmi les procédures de contrôle et d'audit interne, 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.

249. 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.

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

- <u>Définition et objectifs</u>

251. 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.

- <u>Articulation avec les contrôles comptables en place</u>

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

253. 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.

254. 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'organisation.

[8] L'article 47-2 de la Constitution consacre les principes de sincérité, de régularité et d'image fidèle pour toutes les administrations publiques.

255. 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

256. 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

257. 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).

258. 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.

259. 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.

260. 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.

261. 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.

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

263. 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'action.

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

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

266. 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 d'atteintes à la probité) et de l'application des contrôles comptables anticorruption de premier niveau et de deuxième niveau.

- Traitement des anomalies constatées

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

268. 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.

269. 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.

270. 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.

4. Régime disciplinaire

- **Définition**

271. Le régime disciplinaire regroupe l'ensemble des mesures qu'une organisation se réserve le droit de prendre dans le cadre d'un comportement qu'elle considère fautif.

272. Sont notamment considérés comme une faute de nature à justifier une sanction disciplinaire, un manquement aux obligations légales ou un agissement contraire au code de conduite anticorruption.

- **Principe de gradation des sanctions**

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

- **Mécanisme**

274. L'engagement de l'instance dirigeante dans la maîtrise du risque d'atteintes à la probité implique, lorsque des manquements aux devoirs d'intégrité et de probité des personnels sont constatés, d'engager une procédure disciplinaire et de mettre en œuvre des sanctions disciplinaires proportionnées.

275. 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.

276. 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. Un signalement au procureur

de la République sur le fondement de l'article 40 du code de procédure pénale peut être réalisé parallèlement.

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

277. 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.

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

- **Communication interne**

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

II.5) Contrôle et évaluation des mesures et procédures composant le dispositif de prévention et de détection des atteintes à la probité

1. Objectifs et modalités

280. Afin de s'assurer de l'adéquation et de l'efficacité des procédures de prévention et détection des atteintes à la probité, l'organisation 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.

281. 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.

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

283. 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.

284. La pertinence et l'efficacité des mesures et procédures composant le dispositif anticorruption sont régulièrement évaluées par des contrôles de troisième niveau. Ces audits internes visent à s'assurer que le dispositif de prévention et de détection des atteintes à la probité est conforme aux exigences de l'organisation, 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

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

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

Procédure	Points d'attention
Cartographie des risques d'atteintes à la probité	- s'assurer régulièrement de la pertinence du périmètre de la cartographie, de la méthodologie mise en œuvre, du déploiement des plans d'actions y afférents ;

	- analyser les insuffisances constatées et notamment les incidents survenus afin de mettre à jour la cartographie.
Code de conduite et politiques/procédures annexées	- s'assurer de la mise en œuvre effective des procédures (par exemple, en matière d'acceptation de cadeaux et invitations), par des contrôles *a priori* et des contrôles *a posteriori* 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	- 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.
Evaluation des tiers	- s'assurer de la mise en œuvre effective des mesures de vigilance par des contrôles a priori et des contrôles a posteriori 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 de 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.

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

288. 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.

289. 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

290. 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.

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

ANNEXE

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

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

Elle recommande aux acteurs publics de prendre en considération ces situations, qui ne sont pas exhaustives, au cours de l'analyse de leurs risques. En miroir, elle a également identifié certaines mesures de prévention et de détection, ainsi que de bonnes pratiques, de nature à les atténuer.

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 particulier 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

- ✓ 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.
- ✓ Prévoir une obligation de compte-rendu de l'usage de la subvention attribuée.
- ✓ 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.

- ✓ Mettre en place un contrôle, éventuellement par sondage, de l'instruction des dossiers de demande de subvention.
- ✓ 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…
- ✓ 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.

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.
- ✓ Organiser une rotation régulière des agents occupant des postes particulièrement exposés aux atteintes à la probité.
- ✓ 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.

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 une organisation en contrepartie d'une somme qu'elle 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 organisations 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.
- ✓ Non application des pénalités prévues au marché.
- ✓ Etablissement 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 adaptés (seuils), stricte application des critères justifiant le recours aux procédures dérogatoires.
- ✓ Consultation : donner le même niveau d'informations 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 procédure adaptée.
- ✓ Exécution : porter une attention particulière au service fait, réaliser des contrôles réguliers sur les prestations ou travaux réellement réceptionnés (volume, qualité).