RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

AFA
Agence Française Anticorruption

THE FRENCH ANTI-CORRUPTION AGENCY GUIDELINES

Notice on the French Anti-Corruption Agency Guidelines to help Public and Private Sector Entities to Prevent and Detect Bribery, Influence Peddling, Extortion by Public Officials, Illegal Taking of Interest, Misappropriation of Public Funds and Favouritism.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

AFA
Agence Française Anticorruption

Disclaimer

This document is a courtesy translation. Only the French version of the guidelines published in the Official Journal of the French Republic ("Journal officiel de la République française") is the authentic text for interpretation by AFA and the organisations that refer to it.

Notice on the French Anti-Corruption Agency Guidelines to help Public and Private Sector Entities to Prevent and Detect Bribery, Influence Peddling, Extortion by Public Officials, Illegal Taking of Interest, Misappropriation of Public Funds and Favouritism

NOR: ECOZ2035293V

Version dated 4 December 2020

Contents

I. General provisions

I.1) Purpose

1. According to the provisions of the first paragraph of Article 3(2°) of the Transparency, Anti-Corruption and Economic Modernisation Act 2016-1691 of 9 December 2016, known as the Sapin II Act (referred to hereinafter as "the Act", unless otherwise specified), the French Anti-Corruption Agency (AFA) "*shall draft guidelines to help public and private sector entities prevent and detect bribery, influence peddling*, *extortion by public officials*, *illegal taking of interest, misappropriation of public funds and favouritism*".

2. All of these illicit acts are defined under Title III of Book IV of the Criminal Code, in Section 3 of Chapter II ("breaches of the duty of honesty"), and in Section 1 of Chapter V ("bribery of persons not holding public office") under Title IV. For the sake of simplification, unless otherwise indicated, these guidelines shall refer to all of these offences as "corruption".

3. These guidelines interpret the provisions of the Act dealing with arrangements for preventing and detecting these offences. The guidelines are intended to update and supplement the previous guidelines on this subject issued in December 2017, building on AFA's experience after three years of performing its tasks.

4. The Act, the implementing decrees, these guidelines and the guides posted to the AFA website constitute the French anti-corruption policy framework. This framework contributes to the implementation of France's international commitments in the fight against corruption.

5. These guidelines, which come into force the day after they are published, shall replace the previous guidelines published in the official journal of the French Republic on 22 December 2017.

I.2) Scope

6. The guidelines define the procedures for implementing programmes for preventing and detecting corruption (hereinafter "anti-corruption programmes") that all public or private sector entities, incorporated under French or foreign laws (hereinafter "organisations") and doing business in France or abroad may deploy in accordance with their risk profile, regardless of their size, legal structure or status, business sector, budget, turnover, or number of employees.

7. The guidelines are also intended to help organisations that are required to deploy an anti-corruption programme to comply with the Act.

I.3) Legal force

8. These guidelines are not legally binding on the target organisations. The organisations mentioned in Paragraph 7 are free to adopt other methods, provided that implementation of such methods results in compliance with the Act.

9. AFA cites the guidelines when it performs its advice and monitoring tasks. AFA shall not cite these guidelines in its audits until six months after their entry into force.

10. These guidelines are binding on AFA in its auditing activities, meaning that the organisations mentioned in Paragraph 7 can invoke the guidelines if they have decided to comply with them.

11. This means that, in the event of an AFA audit, an organisation mentioned in Paragraph 7 stating that it has followed these guidelines shall benefit from a prima facie presumption of compliance. This presumption may be reversed only if AFA demonstrates that the application of the guidelines was ineffective, incorrect or incomplete.

12. An organisation mentioned in Paragraph 7 that decides not to follow some or all of the methods recommended by the guidelines cannot be presumed to be in compliance with the Act prior to an audit. However, if AFA disputes some or any of the organisation's measures during an audit, it is up to the audited organisation to show that its choices enable it to meet the requirements of the Act.

I.4) Core principles

13. Hereinafter, the term "anti-corruption programme" shall denote all of an organisation's measures and procedures for raising awareness, preventing, detecting and sanctioning some or all of the offences mentioned in **Erreur ! Source du renvoi introuvable.**.

1. Principle of proportionality and scope of intervention

14. Organisations adapt these guidelines in accordance with their risk profile, which is shaped by different parameters, such as business activities, competence or type of product or service provided, along with governance structures, organisational structures, size, business sector, locations and dealings with different categories of third parties.

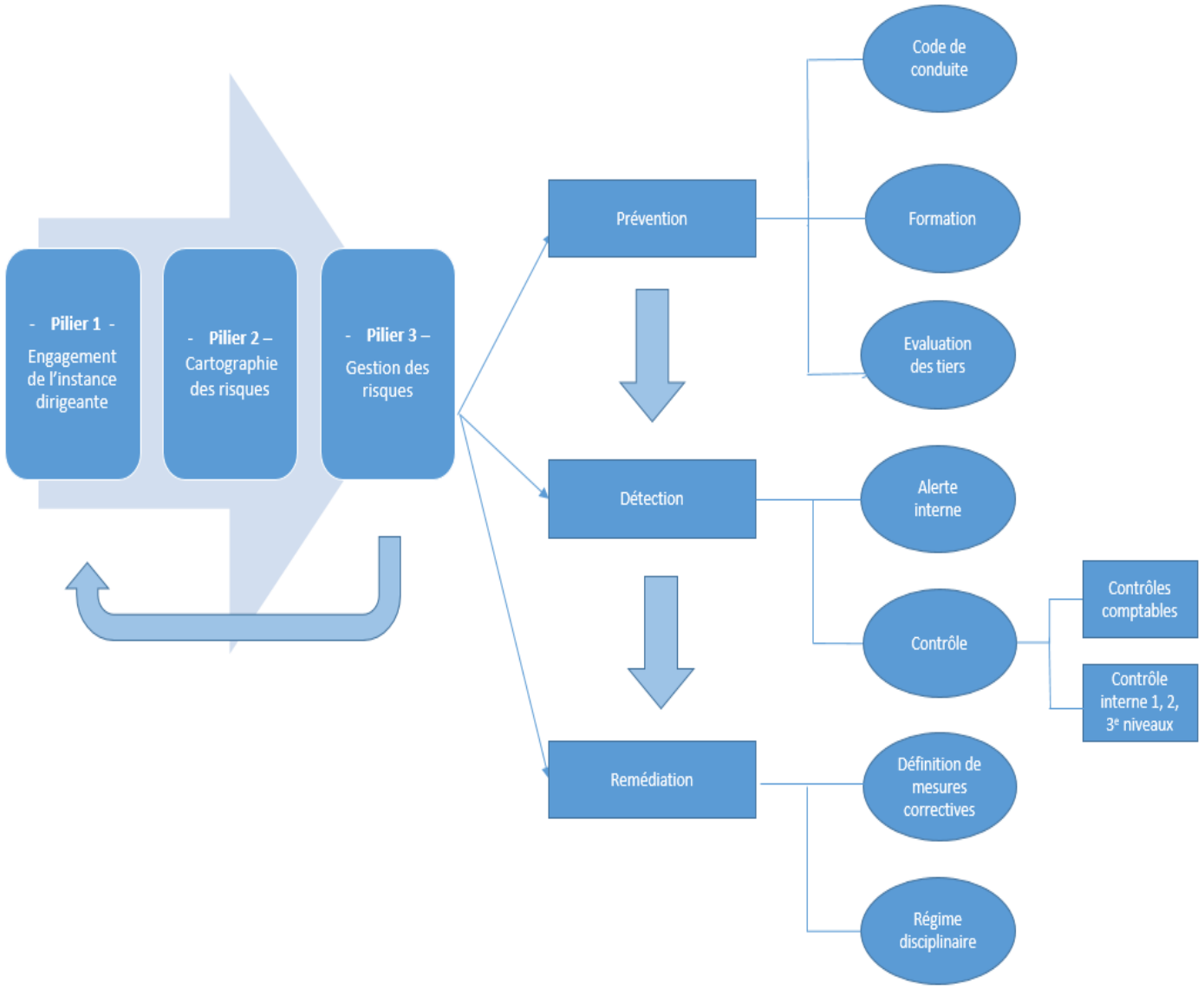
15. Organisations that control other entities ensure the quality and effectiveness of the anti-corruption programmes deployed by all of the entities under their control.

2. Three inseparable pillars

16. An anti-corruption programme is based on three inseparable pillars:

- The first pillar is the commitment of senior management to corruption-free performance of the organisation's tasks, competence or business. This requires senior managers to:
  - to show exemplary personal behaviour in both word and deed with regard to integrity and honesty;
  - to promote the anti-corruption programme through personal communication;
  - to implement the necessary resources to build an effective and efficient programme.
  - to be accountable for proper oversight of the programme;
  - to comply with the programme in their own decision-making;
  - to ensure that appropriate and proportionate sanctions are imposed in the event of violations of the code of conduct or conduct that could qualify as corrupt.
- The second pillar is using risk mapping to raise awareness of the entity's exposure to corruption risks;
- The third pillar is management of the identified risks by means of effective measures and procedures to prevent and detect any behaviours or situations that violate the code of conduct or that could constitute corruption, and to impose the relevant sanctions. This risk management also includes monitoring and assessment of the effectiveness of the measures and procedures concerned.

Overview



1st Pillar – Senior management's commitment **2nd Pillar** – Risk mapping **3rd Pillar** – Risk management	Prevention	Code of conduct Training Third-party due diligence
	Detection	Whistleblowing Internal control → Accounting controls 1st, 2nd,3rd lines of defence
	Corrective action	Definition of corrective measures Disciplinary rules

First pillar: senior management's commitment

17. Senior management includes the people at the head of the organisation who are responsible for its management in accordance with the corporate bylaws and the standards in force. Senior management initiates the implementation of the anti-corruption programme, validates its design and deploys and monitors the programme.

18. If senior management performs its tasks under the supervision or oversight of a non-executive board, that board ensures that corruption risks are properly addressed through the implementation of an appropriate and effective anti-corruption programme.

19. The commitment of senior management to corruption-free performance of the organisation's tasks, competence or business constitutes the basis of any anti-corruption programme.

20. This commitment is shown not only by senior management's determination to prevent and detect any corruption within the organisation, but also by allocation of appropriate resources.

21. Senior management deploys appropriate resources proportionate to the organisation's risk profile in order to design, implement and monitor the measures and procedures that constitute the anti-corruption programme.

22. Senior management is personally responsible for the design, deployment and monitoring of the programme, even if it delegates implementation to staff member. In the latter case, the staff member concerned must be able to report directly to senior management.

23. Senior management ensures that the staff member and any personnel working under them for the execution of their tasks have the necessary knowledge based on their experience or training, and adequate powers to perform their duties and access the information required to fulfil their functions.

24. Senior management ensures that the programme in place is operating properly by examining the audit findings it receives about the various measures and procedures of the programme.

25. Senior management is personally involved in the operational implementation of certain measures and procedures constituting the anti-corruption programme, for example, when the corruption risk map is validated, when decisions are made following third-party due diligence or when determining the penalties to be imposed for code of conduct violations or for acts that could be qualified as corruption.

26. Senior management communicates about its anti-corruption programme, both internally and to the third parties with which it is planning or continuing to maintain relationships. It stresses its own unwavering commitment to ethics and integrity.

27. Senior management ensures that appropriate and proportionate sanctions are imposed for code of conduct violations or for acts that could be qualified as corruption.

Second pillar: corruption risk mapping

28. Corruption risk mapping is the cornerstone of the anti-corruption programme. It is the basis for defining the other prevention and detection measures. It is based on identifying, assessing and ranking each organisation's specific corruption risks.

29. It contributes to a risk-based approach that requires understanding and assessing the organisation's corruption risks, as well as implementing appropriate and proportionate measures and procedures to manage these risks effectively.

30. Risk mapping consists of regularly updated documentation intended to make the organisation aware of its corruption risks.

31. It is the result of detailed analysis of the organisation's processes. The map is drawn up using a method that ensures a reasonable assurance that the risks identified are a faithful reflection of the organisation's actual risks. The risks are assessed for their true severity, correctly ranked and addressed by action plans to ensure that they are effectively managed.

32. Senior management validates the risk map, after it has been submitted to the non-executive governing body, as the case may be. The risk map should be validated prior to implementation and after each update.

33. The risk map may be incorporated into a broader risk map that also complies with the terms of paragraphs 28 to 32.

Third pillar: corruption risk management measures and procedures

- **Systematic nature of the anti-corruption programme**

34. The design, deployment and implementation of the anti-corruption programme should be appropriate for the risks that the organisation has identified, evaluated and prioritised.

35. The measures and procedures are appropriate for the risks that they are intended to manage. They aim for three objectives: risk prevention, risk detection and, when necessary, remediation of any shortcomings found.

- **Corruption prevention procedures and measures**

  - **The code of conduct and the related procedures and policies**

36. The code of conduct, or any equivalent document, regardless of its title, sets out the ethical rules applying to management and staff. It refers to the risk map to define and illustrate the various types of prohibited behaviours that could constitute corruption.

37. It is clear, straightforward and unequivocal.

38. It starts with a preface by senior management stressing the importance it places on fighting corruption within the organisation.

39. The code of conduct is binding in every way on the organisation's staff, in accordance with the applicable standards. If the organisation has rules of procedure, the code of conduct is incorporated into these rules. Where appropriate, it is the subject of a consultation procedure with the relevant entities, authorities and departments.

40. Other ethics and good practice policies may be incorporated into the code of conduct or appended to it, such as policies on gifts and entertainment, sponsorship, lobbying, managing conflicts of interest, entertainment expenses, holding multiple jobs, or any other procedures contributing to the fight against corruption.

41. The code of conduct and the related procedures and policies constitute a coherent whole that is easily accessible for the organisation's staff. It may be communicated to third parties, as the case may be, following appropriate procedures for the purpose of protecting any confidential information that it may contain.

- **Awareness raising and training about corruption risks**

42. Awareness raising for all of the organisation's staff may be part of a general initiative.

43. Executives and the most highly exposed staff must take mandatory training, adapted to their activities and their potential risks. The corruption risk map is used to identify the target trainees and the content of the training.

44. The trainees must be able to understand the architecture of the anti-corruption programme, to identify the specific risks that they encounter in their jobs and the procedures and measures that apply to such situations. These objectives must be attained, regardless of the awareness-raising and training procedures applied.

45. Indicators for monitoring and testing trainees must be defined for the purpose of oversight of the training.

- **Third-party due diligence**

46. Insufficient third-party due diligence with regard to planned or current relationships could expose the organisation to the risk of more or less direct implication in corruption offences that could harm its reputation, adversely affect its business development, and engage the liability of the organisation or its senior management.

47. The purpose of third-party due diligence is to manage these risks by assessing the risk incurred by the organisation in dealing with any third party, including customers, service providers and suppliers, merger and acquisition targets, users and partners. Potential corruption risks can arise in relationships with any individual or legal entity.

48. The nature and thoroughness of the due diligence and the information to be gathered are defined for various uniform groups of third parties, meaning third parties with comparable risk profiles, as determined by the risk map. Consequently, the groups of third parties deemed to be risk-free or low-risk may require no due diligence or simplified due diligence, whereas groups deemed to present greater risks will require more thorough due diligence.

49. Due diligence can be performed using different means, ranging from simple open-source searches to in-depth investigations, or self-assessment questionnaires sent to the third parties.

50. Due diligence findings enable senior management to assess the appropriateness of initiating a relationship with a third party, continuing a relationship or, when necessary, ending a current relationship with the appropriate due diligence measures[1].

51. Dealings with high-risk third parties are subject to enhanced due diligence measures to ensure the security of the transactions concerned. Surveillance of the relevant financial flows and the proper performance of the tasks given to these third parties contributes to this security.

[1] Subject to compliance with the provisions governing this process in the case of public sector entities.

52. Specific clauses that are in compliance with legal requirements may be included in contracts to rescind or not renew business relationships in the event of cases of corruption or failure to comply with the organisation's directives in these matters.

- **Corruption detection procedures and measures**

  - **Internal whistleblowing system**

53. The internal whistleblowing system is used to gather reports of behaviours and situations that are code of conduct violations or potentially constitute corruption.

54. The whistleblowing system must be appropriate for the nature of the organisation's risks, without prejudice to the specific rules for different types of organisations that are likely to shape internal whistleblowing systems. The system must make it possible for whistleblowers to make good faith reports and ensure that they are protected.

55. The system may be managed within the organisation or by a third party under contract, provided that the third party is competent to process reports properly and maintain confidentiality.

56. The whistleblowing system may have one or more channels for submitting reports, ranging from a dedicated e-mail address to management software, and even a dedicated ethics platform for some organisations. These reporting channels must be easily accessible for the organisation's permanent and temporary personnel. It may also be helpful for organisations to make these channels accessible for the third parties that they deal with.

57. The whistleblowing system may also stipulate that a whistleblower should report to their superior first. The superior should be able to guide and advise the whistleblower, as the case may be, unless the superior is the person whose behaviour is implicated.

58. The whistleblowing system is secure and access privileges are restricted to those staff members authorised to receive and process the reports.

59. Reports may be submitted anonymously. The system must make it possible to continue dialoguing with the whistleblower while maintaining anonymity (for example, using an anonymous email address or a post office box).

60. The organisation specifies the procedures for processing reports received, such as:

- the contact person designated to receive reports within the organisation and, the person responsible for processing reports, if it is not the same person;
- the provisions made to ensure maintain the confidentiality of the whistleblower's identity, the contents of the report and the persons implicated, even when the investigation or processing of the report require communications with third parties;
- The procedures that the whistleblower needs follow to provide any information or documents to back up the report;
- The business information and documents that may be used in an internal investigation;
- The provisions for notifying the whistleblower of receipt of the report and, as the case may be, of the admissibility of the report, along with the processing time and any action taken to follow up the report;
- If the report does not give rise to any further action, the provisions for destroying any information on file that could be used to identify the whistleblower or the persons implicated, within two months of closing the investigation;
- If automated processing of reports is implemented, the provisions for ensuring compliance with data protection standards;

- Implementation of indicators to assess the quality and effectiveness of the whistleblowing system (including the number of reports received, shelved or processed, processing times, problems raised). These indicators are submitted to senior management, along with the most critical reports.

▪ Control system

61. The organisation sets up an appropriate internal control and audit system that is proportionate to its corruption risks.

62. The system serves several purposes:

- Preventing and detecting corruption, as the case may be;
- auditing the effective, compliant and efficient measures and procedures for preventing and detecting corruption and defining the appropriate corrective recommendations or measures to improve them.

63. Ideally, the control system may include up to three autonomous lines of defence.

64. The purpose of the first line of defence is to conduct preventive controls prior to implementing decisions and transactions to ensure that the tasks that are inherent in an operational or support process are performed in compliance with the organisation's procedures. The first-line-of-defence controls are performed by the operational or support staff, or by their superiors.

65. The purpose of the second line of defence is to conduct detective controls at prescribed intervals or randomly on some or all of the decisions or transactions to ensure that the first-line-of-defence controls have been properly performed and that the overall anti-corruption programme is functioning properly.

66. The purpose of the third line of defence (or "internal audit") is to perform periodic controls to ensure that the control system complies with the organisation's requirements and is implemented effectively and kept up to date. The persons responsible for third-line-of-defence audits are independent. They are appointed by and report directly to senior management.

67. The findings of second- and third-line-of-defence controls and the implementation of corrective measures are reported regularly to senior management.

68. The organisation may incorporate its internal control and audit system of the anti-corruption programme into a broader risk management system, subject to compliance with the provisions of paragraphs 61 to 67.

69. Accounting control and audit procedures may be the preferred means of detecting corruption as part of the internal control and audit procedures.

70. Accounting controls ensure that the books, ledgers and accounts are not used to conceal corruption. These procedures focus on the high-risk situations highlighted in the corruption risk map. If the organisation has no such controls, it needs to define and deploy them.

71. The segregation of responsibilities for verifying services rendered, payment requests, payment authorisation and actual payments contributes to corruption prevention, without prejudice to the effect any specific standards or regulations applying to different types of organisations on their accounting control.

72. Ideally, the organisation implements three lines of defence for accounting control, following the same procedures as for internal control defined above. The three lines of defence are first- and second-line-of-defence accounting controls and accounting audits.

73. Accounting controls may be performed by the organisation's own accounting and financial control function, or by a competent external auditor.

74. The organisation may incorporate its accounting control and audit system for preventing and detecting corruption into a general accounting control and audit system, provided it complies with the provisions of paragraphs 69 to 73.

- **Managing any problems found**

75. Any problems found when performing controls, or under other circumstances, give rise to the definition of corrective measures that may be incorporated into an action plan.

76. Action plans defined in this manner state the problems identified, detail the remedial actions to be performed, designate the persons responsible for implementing the actions and set the timeline.

77. Progress on action plans is monitored and reported to senior management on a regular basis.

78. Senior management imposes the appropriate sanctions for failure to comply with the code of conduct and any appendices or for any instances likely to be qualified as corruption.

79. The sanctions imposed are recorded to identify the causes and to prevent repetition.

80. Senior management communicates within the organisation about the incidents and the related sanctions, while maintaining anonymity and ensuring that the persons sanctioned cannot be easily identified.

81. When senior management is not required to implement the provisions of Article 40 of the Code of Criminal Procedure by notifying the relevant prosecutor of corruption cases that could constitute criminal offenses, it remains free to do so, if it deems it appropriate, or to file a complaint, as the case may be.

- **Retention and archiving of measures and procedures and their elaboration method**

82. The organisation implements a record retention and archiving system for the documents and information from its anti-corruption programme to ensure an audit trail is created. This system complies the data protection and privacy standards. This is a particularly necessary precaution if the methods used by the organisations mentioned in paragraph 7 do not correspond to the methods suggested in these guidelines.

83. The methods that the organisation uses to elaborate its anti-corruption programme and updates to the programme are also retained and archived.

84. These records are retained for periods that vary depending on the nature of the information they contain. Under current legislation, and the General Data Protection Regulation (GDPR) in particular, an organisation may not retain personal data indefinitely. The adaptations of the general provisions are explained below.

II. Adaptation of the general provisions applicable to companies subject to Article 17 of the Act

85. The following provisions explain the variations of the provisions set out in paragraphs 13 to 84 of these guidelines in the case of organisations subject to Article 17 of the Act.

86. For the purposes of Article 17 (I) of the Act, managers of the organisations listed in paragraph 93 (hereinafter "companies") are required to "*implement measures and procedures to prevent and detect acts of bribery and influence peddling committed in France or abroad*".

87. The measures and procedures listed in Article 17 (II), therefore, concern prevention of only two (bribery and influence peddling) of the six offenses listed in Article 1 of the Act. This means prevention and detection of these two offenses could be addressed by implementing identical measures and procedures, since the offenses are strictly the same in terms of the material elements that constitute them. In cases of passive corruption, they differ only by the position of the perpetrator.

88. Above and beyond the legal stipulations, organisations are advised to have anti-corruption programmes that address a broader range of risks that are not explicitly mentioned in the legislation, but would could lead to or follow the offenses mentioned in the Act. This is particularly the case for the offenses of forgery or misuse of corporate assets, which warrant accounting control, or the offenses of concealment or laundering related to all of the offenses stipulated in Article 1 of the Act.

89. Unless otherwise indicated, the offenses mentioned in paragraph 87 shall both be called "bribery" in the rest of Section II of these guidelines.

90. Semi-public companies and public industrial and commercial establishments that reach the threshold set in Article 17 are still subject to the requirements set out in Article 3 (3°) of the Act. Consequently, in addition to the risks of bribery and influence peddling, their anti-corruption programme must deal with the risks of extortion by public officials, illegal taking of interest, misappropriation of public funds and favouritism.

91. Companies that control other entities, such as subsidiaries, branches and agencies, are encouraged to establish procedures and internal control to ensure the quality and effectiveness of the anti-corruption programme or programmes deployed in all of the entities under their control.

II.1) First pillar: senior management's commitment

92. Article 17 of the Act requires senior management "*(…) to take measures to prevent and detect acts of bribery or influence peddling committed in France or abroad in accordance with the provisions of II)*". Failing that, it may be liable to the decisions of the AFA Sanctions Committee. Therefore, it is in senior management's interest to ensure that an appropriate anti-corruption programme is implemented in every area of the company's business.

1. Definition of senior management

93. The following persons constitute senior management under the terms of Article 17 of the Act:

- Chairs, general managers and managers of companies with their registered office in France, having more than five hundred employees and turnover in excess of €100 million;
- Chairs, general managers and managers of companies belonging to a group of companies with a parent company having its registered office in France, more than five hundred employees and consolidated turnover in excess of €100 million;

- Chairs, general managers and managers of government-funded industrial and commercial institutions with more than five hundred employees and turnover in excess of €100 million, or belonging to a government-funded group with more than five hundred employees and consolidated turnover in excess of €100 million;
- Members of the management boards of limited liability companies governed by Article L. 225-57 of the Commercial Code with more than five hundred employees, or belonging to a group of companies with more than five hundred employees and turnover or consolidated turnover in excess of €100 million

94. A "group of companies" means a company and its subsidiaries, as defined by Article L. 233-1 of the Commercial Code, or it means a company and the companies it controls, as defined by Article L. 233-3 of the Commercial Code.

95. This definition does not cover members of the board of directors or other supervisory bodies on the whole. Nevertheless, their oversight of the company's activities includes ensuring that the managers' measures to comply with their legal obligations are in place, appropriate and effective. AFA recommends that companies with such supervisory bodies periodically present their anti-corruption programme and updates to these bodies so that they have all the information needed to ensure that the company complies with Article 17 of the Act.

2. Senior management's responsibility

96. Senior management commits to implementing a zero-tolerance policy for any conduct that could constitute corruption, and promotes and disseminates a culture of integrity within the company and vis-à-vis third parties by making corruption prevention and detection a priority. This is one of the foundations of corruption prevention and detection.

97. Implementing an anti-corruption programme is the responsibility of senior management, which may, as appropriate, delegate operational implementation to an anti-corruption compliance officer, hereinafter referred to as the "compliance officer".

98. Senior management defines the risk management strategy and ensures that it is implemented. In this respect, it is responsible for formally approving the programme and, in particular, the corruption risk map. It ensures that a related action plan is implemented and that suitable resources are provided to conduct and monitor it. Senior management uses indicators and control and audit reports to ensure that the anti-corruption programme is organised, effective and up to date.

99. In addition to implementing the measures and procedures that make up the anti-corruption programme, senior management is encouraged to ensure that anti-corruption measures are integrated into high-risk procedures and policies, such as those concerning human resources management, and sales and purchasing policies:

- With regard to human resources management, senior management ensures that:
  - The process for recruiting and appointing managers and the most exposed staff includes an assessment of their integrity;
  - Managers' initiatives to promote corruption prevention and detection with their teams are encouraged and highlighted. For example, compliance with corruption prevention measures could be considered when setting their annual objectives and evaluating their performance.

- With regard to sales policy, senior management is encouraged to ensure that discounts provided to customers are not used for corrupt purposes.
- Competition between suppliers contributes to managing the risks inherent in the purchasing function.

100. Senior management ensures that disciplinary rules are established and that appropriate sanctions are imposed in corruption cases.

3. Dedicated resources

101. The implementation of an anti-corruption programme calls for senior management to provide human and financial resources that are proportionate to the company's risk profile.

102. These resources must cover:

- The anti-corruption compliance team;
- Use of external consultants or service providers, where appropriate;
- Implementation of such tools as third-party due diligence, internal whistleblowing systems, risk management, monitoring, e-learning, etc.;
- Management of anti-corruption training;
- Production of periodic reports and assessments.

- **Compliance officer**

103. The appointment of a compliance officer may be announced to all staff and formalised by a brief from senior management specifying:

- The tasks assigned, which reflect strategic and organisational choices and the company's characteristics (including business model, business sector and size);
- Guarantees of the compliance officer's independence through their position in the company and their access to senior management, the board of directors and to specialised board committees.
- Coordination with other functions in the company and with other compliance areas;
- Organisation of the anti-corruption compliance function within the company, including the material and human resources allocated to the function.

104. Senior management ensures that the compliance officer has the resources needed to perform their tasks, coordinate with the functions concerned and report to senior management.

105. In the case of a company organised around a central body, such as a parent-company-and-subsidiaries arrangement, the compliance officer should be appointed at the central level, with correspondents for each subsidiary, country or organisational unit, for example.

106. The officer may urge subsidiaries to implement anti-corruption programmes and help them to do so by disseminating common methodologies and policies, to be adapted as necessary to suit local constraints (size, specific identified risks, choices made for the organisation of the compliance function, regulations, etc.).

107. The compliance officer may set up an anti-corruption compliance network with their compliance contacts in the company to help design, deploy and control anti-corruption programme(s). The network facilitates the communication of questions and, where necessary, whistleblower reports, as well as sharing experiences. In this way, the network helps improve the company's anti-corruption programme(s).

108. Senior management ensures that the compliance officer always has:

- Access to any information useful for the performance of their tasks, providing a true and fair view of the company's activity;
- Independence from the company's other functions and the capacity to have a real influence on these other functions;
- Access to senior management to ensure voice and support.

109. Irrespective of their position in the company, it is critical for the compliance officer to have direct and regular dealings with senior management and easy access to the board of directors.

110. In addition to their recurring tasks, the compliance officer is involved in implementation of strategic projects and decisions made affecting the structure of the company, such as signing new contracts, mergers and acquisitions, major investments, seeking or engaging in new partnerships, and designing and marketing new products or services.

111. The independence of the compliance officer does not imply the absence of supervision. For this purpose, the compliance officer reports on their activity to senior management.

112. Senior management ensures that the compliance officer has the necessary competence, including:

- The ability to perform a cross-cutting function;
- Knowledge of regulations relating to anti-corruption compliance, as well as knowledge of the

company's activities and risk management techniques. This knowledge may have been acquired through training or job experience.

- **An appropriate internal and external communication policy**

113. The company engages in broad-based communication aimed at all staff about its bribery prevention and detection policy.

114. The in-house communication about the anti-corruption programme is appropriate for the company's structure and activities and necessarily covers the code of conduct, anti-corruption training and the internal whistleblowing system.

115. The company also communicates about its anti-corruption policy to external partners via appropriate means with a view to protecting its staff from illicit solicitation.

II.2) Second pillar: risk mapping

116. Under the provisions of Article 17 (II,3) of the Act, risk mapping takes the form of "*regularly updated documentation for the purpose of identifying, analysing and ranking the company's exposure to risks of external solicitations for the purpose of bribery, in accordance with the activity sectors and locations where the company does its business.*"

117. Interpretation of the various provisions of Article 17, and Article 17(I) in particular, implies that the companies governed by the article must produce not only a map of bribery risks, as specified by the Act, but a map of influence peddling risks as well. A literal interpretation of Article 17(II,3) would undermine the effectiveness of the overall programme, since the other measures, which are all derived from the risk map, are also aimed at preventing and detecting influence peddling. This aim is implicit in the code of conduct, accounting control procedures and training programme, and it is explicit in the whistleblowing system, third-party due diligence procedures, etc.

118. Risk mapping is a key tool for awareness of corruption risks. It is used by companies to engage in and formalise in-depth examination of their risks and to create the right conditions for improving their management of those risks. Risk mapping is conducted to protect against risks and their potential reputational, legal, human, economic and financial repercussions.

119. A corruption risk mapping exercise requires:

- Knowledge of the company's scope and its activities, including the managerial, operational and support processes[2] required for these activities. Such knowledge is a prerequisite for thorough analysis of processes providing reasonable assurance that the map is a true and fair view of the company's actual risks in its dealings with third parties. Each company produces its own risk map, which is specific to that company and therefore cannot be transposed directly to another company.
- Identification of the roles and responsibilities of the players concerned at all levels within the company.

1. Risk mapping objectives

120. Risk mapping starts with an objective, structured and documented analysis of the company's exposure to corruption risks in the course of its activities. This is the result of an analysis of all of the company's processes that involve dealing with third parties, along with the identification of corruption risks at every stage in these processes.

121. The risk map provides senior management with the necessary information to implement effective prevention and detection measures that are proportionate to the issues that the map has identified and appropriate for the company's activities.

122. The risk map enables the company to manage its risks effectively with the preventive, detective and corrective measures and procedures discussed below. The lessons learned from the implementation of these measures and procedures are then fed back into the corruption risk map and its updates. All of these interactions are part and parcel of a systemic approach to corruption risk mapping and to the design and implementation of risk management measures and procedures.

[2] In the context of these guidelines, the notion of process covers a set of correlated or interacting tasks aimed at meeting a managerial, operational or support need.

2. Risk map characteristics

123. The risk map is complete when it covers:

- The company's managerial, operational and support processes for its dealings with third parties. The map captures corruption risks, with due consideration of the specific features of each company, including activity sectors, locations, competition and the regulatory context, types of third parties, business model, value chain, activities and processes, internal organisation and decision-making circuits;
- And the scope of the company's business. For example, if a company has *de jure* or *de facto* control of other entities, as in the case of a parent company and its subsidiaries, its risk map considers the risks inherent in the activities of the companies under its control. For this purpose, controlled companies submit their corruption risk maps and the associated action plans to the parent company, which monitors the production of risk maps. It may be helpful to aggregate subsidiaries' risk maps with the parent company's risk map. The latter provides an overview of the different entities' risks and the associated action plans.

124. The risk map is formalised, i.e. it takes the form of written and structured documentation with a detailed description of the methods used to produce the map, the measures taken to manage the risks and the roles and responsibilities of the different stakeholders.

125. Depending on the company's activities and organisation, the risk map may be organised by activity, process, entity or location.

126. The risk map is to be used as a risk steering tool and must facilitate external assessment (in the event of administrative audits or legal action) of the appropriateness of the anti-corruption programme.

127. The risk map is dynamic given the need for periodic reassessment of risks, particularly whenever a significant change occurs within the company. This updating places mapping within a continuous improvement process used by companies to enhance their risk management.

3. Risk mapping steps

128. Risk mapping starts with an objective, structured and documented analysis of the company's exposure to corruption risks in the course of its activities. The description identifies the potential impact of the risks (severity) and the likelihood of occurrence (frequency), factors that may exacerbate them (aggravating factors) and responses under the existing risk management system or an action plan.

129. For the purpose of identifying, assessing and managing corruption risk, we recommend following six steps.

130. Pre-existing work may be built on in the case of companies that have already conducted risk mapping exercises within a broader context or for risks other than corruption risks.

Step 1: Roles and responsibilities of risk mapping stakeholders

131. Companies can usefully assign roles and responsibilities as follows:

- Senior management promotes the risk mapping exercise and provides the compliance officer with the means for implementing it. It approves the basic principles of the risk management strategy and ensures that the chosen action plan is implemented.
- The compliance officer coordinates the risk mapping exercise, guiding the company in the identification of its processes and corruption risks, in the ranking of these risks and in the

definition and implementation of risk management measures. The compliance officer is responsible for drawing up the corruption risk map and submits each risk map update and action plan monitoring report to senior management.

- Managers of decision-making, operational, accounting and other support processes each contribute to the development and updating of the risk map in their area of responsibility. They are responsible for identifying risks that are specific to their activities in accordance with the company's anti-corruption procedures.
- The risk manager, when the company has one, also contributes to defining the methodology for identifying, analysing, ranking and managing corruption risks. The compliance officer and the risk manager work in close collaboration on this point. The corruption risk map may be produced at the same time as a map of other risks, such as operating, accounting and fraud risks in order to optimise the use of resources. In this case, it is important to draw a clear distinction between corruption risks and other risks during the risk mapping exercise.
- Staff members, by virtue of their practical experience of the company's processes, contribute to the mapping exercise by reporting on the factors specific to their functions and the risks incurred in order to take appropriate steps to identify, assess and rank these risks.

132. The company ensures that the risk mapping exercise captures the risks inherent in the activities of all of its staff members, regardless of their status, along with executives, directors and managers.

Step 2: Identification of risks inherent in the company's activities (process identification and risk scenarios)

133. Identification of the company's risks entails a detailed analysis of its processes:

- In the first step, the company may identify its processes on the basis of its activities, building on a pre-existing map of its processes where applicable. At this stage, the company is careful not to come to a foregone conclusion regarding the findings of the risk mapping exercise by drawing up an ex-ante list of processes deemed the most representative or most exposed to risks.
- In the second step, the company consults with staff at all levels of the hierarchy and from all parts of the company about the processes identified. These consultations may take the form of workshops, interviews or questionnaires. The staff members are chosen for their operational familiarity with the processes in order to identify the risk scenarios that the company encounters in its activities, which may be related to specific business lines, subsidiaries or locations.

134. The aim is to take an accurate inventory that can be used to identify in detail and document the risk scenarios that are specific to the company. Although the ideas shared in these discussions could draw on a list of risks scenarios drawn up in advance, such a list cannot be allowed to pre-determine the nature, number and classification of the risk scenarios chosen following the discussions.

135. Participants in the discussions speak freely and a written summary lists all of the risk scenarios and risk factors identified.

136. Risk scenarios are identified in consideration of the company's business environment, which may be affected by:

- The countries where the company does business,
- Its business sectors;

- The nature of its operations, particularly strategic operations (mergers and acquisitions, asset sales, new strategic partnerships, etc.)
- The nature of the third party, its business sector, the type of relationship (direct or indirect), the presence of politically exposed persons, the level of economic dependence;
- The length of the sales cycle and competitive pressures, compensation arrangements for sales people;
- Payment terms and means;
- Past incidents involving the company: including incidents revealed by internal audits or internal whistleblower reports that gave rise to disciplinary sanctions;
- Incidents that gave rise to court rulings concerning companies with comparable risks.

Step 3: Assessment of gross risks

137. The purpose of this step is to assess the company's vulnerability to each risk scenario identified in step 2. The aim here is to identify the company's "gross" risks, i.e. the risks considered before any management measures are taken.

138. This vulnerability is assessed using the following three indicators: impact, frequency and aggravating factors.

139. An analysis is conducted of the impact of each identified risk scenario. Impacts may be reputational, human, financial, economic or legal. Of course, a single risk scenario may involve more than one type of impact.

140. Probability is determined using the fullest, most suitable information for the specific nature of the identified risk (e.g. past incidents).

141. Aggravating factors are assessed by applying severity coefficients. For example, in the case of companies with international activities, this coefficient captures the impact of geographic presence at the gross risk assessment stage.

142. Consultations held to identify the risks can be helpful for assessing those risks. Gross risk assessments, whether it is based on such consultations or not, are made on the basis of a uniform methodology. In particular, the company ensures that the gross risk assessments for different business lines, subsidiaries or locations can be aggregated coherently.

Step 4: Assessment of net or residual risks

143. This step assesses the extent of risk management by the company in order to determine its "net" or "residual" risks. This consists of re-assessing the "gross" risk scenarios after implementation of existing risk management measures.

144. At this stage of the risk mapping exercise, the effectiveness of the existing risk management measures should be assessed using the audits conducted.

145. Ideally, the identification of existing risk management resources implemented takes place during consultations with staff held to identify the risks inherent in the company's activities (Step 2). The assessment of the effectiveness of these measures and, consequently, the net or residual risks, is the task of the compliance officer, working as needed with the managers of the functions concerned and with the support of the internal audit function and the risk manager, if the company has one.

Step 5: Net or residual risk ranking and preparation of the action plan

146. Once the "net" or "residual" risks have been assessed, a classification emerges by level of risk scenarios.

147. Where these risk scenarios return the same net assessment level, and where the company deems it useful to separate them out to prioritise the actions to be taken, they can be ranked using an objective methodology suited to the company's particular activities based on a combination of different criteria such as country risk, turnover, and the nature and type of relationships with third parties.

148. This ranking of risks is used to distinguish risks deemed to be adequately managed from risks where senior management would like to improve management by enhancing internal control.

149. Once this acceptable risk threshold has been set and documented, the measures to be taken to manage the risks are determined as part of the risk management strategy.

150. An action plan is developed on the basis of these elements. The timetable and procedures for implementation of the action plan, along with the related monitoring and reporting procedures should be the responsibility of specifically designated players. Preparation, formalisation and monitoring of this action plan constitute a prerequisite for the effectiveness of the risk map.

Step 6: Formalising, updating and archiving the risk map

151. All the above-mentioned elements combine to form the risk map. Its presentation is integral to ownership of the map as a corruption risk steering tool. It is up to the company to choose to organise the map by business area, by process, by entity or by location. The map is backed up by an annex that describes how it was produced and the methodology for identifying, assessing, ranking and managing risks.

152. Once a year, the need for possible updates is assessed.

153. Map updates may provide an occasion for the company to adapt its methodology or adopt a new methodology so that the resulting risk map provides reasonable assurance that the risks identified provide a true and fair view of the company's actual risks and that they are assessed at their true level and correctly ranked.

154. It is recommended to retain the following elements that can be used to assess the effective implementation of the risk mapping exercise:

- Records of discussions with the staff concerned (diaries, notes, written summaries);
- The method for calculating "*gross*" risks, and the definitions used;
- The method for calculating "*net*" or "residual" risks, and the definitions used;
- The procedures for identifying and categorising risks;
- The different versions of risks maps submitted to senior management, their approval and the related approved action plans;
- The minutes of the different committee meetings.

155. The different versions of the maps and the related audit trails are dated, referenced and archived.

II.3) Third pillar: Risk management

A- Risk prevention

1. Code of conduct

156. Article 17 (II,1°) of the Act stipulates that the persons mentioned in I shall implement a "*code of conduct that defines and illustrates the various types of proscribed conduct that could constitute bribery or influence peddling*. *This code of conduct is to be incorporated into the company's rules of procedure and, by virtue of this fact, it shall be the subject of consultation with the staff representatives as stipulated in Article L.1321-4 of the Labour Code."*

- **Definition and objectives**

157. The code of conduct, whatever the company calls it, is a document that is an expression of senior management's decision to commit the company to bribery prevention and detection.

158. It recapitulates the company's commitments and principles in this regard. It defines and illustrates the various types of proscribed conduct that could constitute bribery.

- **Scope and communication**

159. The code of conduct is applicable to and binding on all of the company's staff.

160. As an instrument for good governance, the code of conduct is applicable everywhere the company does business, including other countries. The same code may apply to all of the entities in the company, provided that this option does not undermine its effectiveness. If the company does business in other countries, the code of conduct should be adapted as needed to specific local legal requirements, which may result from the application of different anti-corruption standards. Similarly, if the company's lines of business are diverse and present specific corruption risks, the company should adapt its code of conduct for different entities or operational units.

161. Other persons who work with the company and are subject to its rules of procedure must comply with the code of conduct.

162. It may be helpful to communicate the code of conduct to third parties, subject to any adaptations required to protect any confidential information that it may contain. Third parties should be bound to comply with the code of conduct by a contractual clause.

- **Drafting and approval process**

163. The code of conduct is drafted jointly by the compliance officers and qualified company staff.

164. It is approved by senior management, which provides leadership by writing the preface to the code, for example. In this manner, the code promotes the development of a culture of compliance, ethics, integrity and honesty, to guide all staff members in their professional relationships.

165. Senior management promotes the code of conduct and scrupulously applies its principles. Setting the example is key to the staff's ownership and application of the code of conduct.

- **Interaction of the code of conduct and other documents**

166. The code of conduct may refer to "operational" fact sheets (or "processes", or "procedures" relating to the gift policy and conflicts of interest, for example). These guides, which are not part of the code itself, define the operational details of compliant conduct to manage high-risk situations identified by the risk map. It is important for all of these documents to constitute a coherent whole, which is clearly expressed, and understandable and accessible for all staff.

167. The code of conduct may also be incorporated into an "ethics" programme (such as a charter of ethics) that encompasses more than just the fight against corruption, provided that its presentation remains perfectly understandable.

- **Coordination of the code of conduct with the rules of procedure**

168. The code of conduct is incorporated into the rules of procedure in companies that have such rules.

169. If the company is not required to adopt rules of procedure in France or in other countries, the code of conduct is provided to staff or made available to them following procedures defined and retained by the company.

- **Content**

170. The code of conduct should be written or updated after the risk mapping exercise, since the code of conduct describes proscribed conduct based on the risks identified.

171. The Code of Conduct provisions deal with the types of proscribed conduct the staff are likely to encounter in the course of the company's activities. Companies are encouraged to divide the code of conduct into sections on the different types of proscribed conduct.

172. The code of conduct is backed up by relevant illustrations of actual cases.

173. The code of conduct is more than just a collection of best practices. It also stipulates prohibitions of conduct and practices that constitute corruption in the company's specific context. For this purpose, it may deal with gifts and hospitality, facilitation payments, conflicts of interest, sponsoring and patronage, and, as appropriate, lobbying and entertainment expenses.

174. The code of conduct presents the internal whistleblowing system for receiving reports about conduct or situations that violate the code of conduct.

175. The code of conduct provides for disciplinary sanctions for proscribed conduct and, more generally, for conduct that does not comply with the company's commitments and principles on preventing and detecting corruption.

176. The code of conduct names the function that is qualified to answer questions from staff (for example, the compliance officer, compliance or integrity contact person) and the procedures for contacting them (such as a generic address).

177. The code of conduct is written in layman's terms. It is clear, straightforward and unequivocal. It may be translated into one or more languages to make it understandable for foreign staff.

- **Updates**

178. The need for updates to the code of conduct is reviewed periodically, particularly following updates of the risk map. For this purpose, the validity date is shown.

2. Awareness and training

179. In accordance with Article 17 (II,6) of the Act, the persons mentioned in I are required to implement a "*training programme for managers and staff who have the greatest exposure to bribery and influence peddling risks*."

180. The anti-corruption training programme is aimed at all managers, as employees with a certain degree of responsibility within the company, as well as at other company staff who are deemed to have the greatest exposure to corruption risks.

- **Definition and objectives**

181. An effective and appropriate training programme is a vehicle for values and a culture of integrity within the company. It promotes broad dissemination of senior management's commitment to fight corruption and ownership of this commitment by the staff concerned. It may be helpful to incorporate it into a broader awareness programme for all staff.

182. The awareness programme makes staff members better informed and more receptive to the issues presented to them, but the training programme provides the knowledge and competence needed to perform an activity or a task. It is incorporated into the company's general training plan.

183. The anti-corruption training programme must:

- Be coordinated with the other anti-corruption programme measures and procedures. For example: training course on the content of the code of conduct, priority training for individuals identified as being at risk by the risk mapping exercise, training and awareness-raising about the use of whistleblowing systems.
- Address the particular risk exposures of different staff categories.

- **An awareness programme for all staff**

184. Although the risk training programme prioritises managers and staff most at risk, an awareness programme is recommended for all personnel.

185. Awareness actions may focus on:

- The code of conduct, as the expression of senior management's commitment;
- Corruption in general, issues, forms and the disciplinary and criminal sanctions incurred;
- Conduct to be adopted when encountering corruption and the role and responsibility of each individual;
- The internal whistleblowing system.

186. Regardless of the procedures used, the purpose of such awareness actions is to promote awareness of corruption issues within the company and its environment.

- **Compulsory training for managers and staff most at risk**

187. Training for managers and the staff most at risk informs them of both the vigilance required of them in the course of their activities and the conduct to be adopted in high-risk situations. The purpose is to have them assume ownership of the company's anti-corruption programme.

188. The ultimate effect of the training is to reduce the risks identified by the corruption risk map.

189. The staff most at risk are identified using the risk map. These may be, in particular:

- Staff dealing with certain third parties (especially sales and purchasing staff);
- Staff taking part in the implementation of the anti-corruption programme.

190. Training content varies depending on whether it is for managers and staff most exposed to the risks of corruption or other staff categories.

191. The content is adapted to the nature of the risks, the functions performed and the locations where the company does business. It is regularly updated in association with the risk map updates.

192. The purpose of training is to improve understanding and knowledge of:

- Processes and their associated risks;
- Corruption offences;
- Due diligence required and measures to be taken to mitigate these risks;
- Conduct to be adopted when encountering illicit solicitation;
- Disciplinary sanctions incurred in the event of non-compliant practices.

193. The common core of these training courses covers:

- The code of conduct, as the expression of senior management's commitment;
- Corruption in general, issues and forms;
- Applicable legal requirements and the associated sanctions;
- The anti-corruption compliance programme;
- Conduct to be adopted when encountering corruption and the role and responsibility of each individual;
- The anti-corruption whistleblowing system.

194. Specific subjects are also addressed depending on the participants' functions and the specific risks they face. Corruption detection tools may be one subject covered by the training for staff with supervisory responsibilities.

195. Managers and staff who are most at risk receive training during their onboarding process. Regular training is provided throughout the exercise of their duties.

196. Like the code of conduct, the training courses use practical case studies and personalised scenarios tailored to each audience and suited to the risks identified by the corruption risk map.

197. Company staff may be asked to share their experiences in this area, their responses and their conclusions, thereby giving rise to discussion of operational constraints. Simulation exercises could be useful to help them take ownership of the rules in their day-to-day work.

198. The use of tools such as tests to check that participants have properly understood the training courses is to be encouraged. Such tests could be set during the training course or following a certain lapse of time to ensure that the knowledge has been assimilated.

- **Monitoring and control of the training programme**

199. Indicators are set up to monitor the training programme, including in the case of outsourced training. These indicators could include the following items:

  - Percentage of target audience trained;
  - Number of training hours on compliance and the anti-corruption programme.

200. The compliance officer must be notified of training schedules and content, and must also be able to monitor the deployment of the programme and the related indicators.

3. Third-party due diligence

201. Article 17(II, 4) of the Act stipulates that the persons mentioned in I implement "*procedures for assessing the situation of customers, leading suppliers and intermediaries with regard to the risk map*".

- **Definition and objectives of third-party due diligence**

202. The Act requires companies to assess customers, leading suppliers and intermediaries.

203. This due diligence should also cover other categories of third parties that the company may have or wish to initiate relationships with, such as acquisition targets, and sponsorship and patronage recipients

204. The purpose of due diligence is to inform the decision to enter into a relationship with a third party, or to maintain a relationship or end it.

- **Coordination of third-party due diligence and other programmes, including the fight against money laundering and terrorist financing (ML/TF)**

205. Third-party due diligence must be distinct from other vigilance requirements concerning customers incumbent on the persons defined in Article L. 561-2 of the Monetary and Financial Code as part of the fight against money laundering and terrorist financing (Article L.561-1 *et seq.* of the Monetary and Financial Code).

206. However, they may be implemented under a single programme, provided the programme can identify specific corruption risks.

- **Definition of the third-party due diligence mechanism**

207. The nature and thoroughness of the due diligence to be conducted and the information to be collected are determined with respect to the different uniform groups of third parties with comparable risk profiles, as identified by the risk map. Consequently, the groups of third parties deemed to be risk-free or low-risk may require no due diligence or simplified due diligence, whereas groups deemed to present greater risks will require more thorough due diligence.

208. The company may identify all of its third parties. The purpose of this approach is to determine *ex ante* the groups of third parties that the company deems to be most exposed to corruption risks on the basis of the risk map.

209. In each group of third parties requiring due diligence, due diligence is conducted on each third party separately according to its particularities, since the purpose of due diligence is to appraise the specific risk associated with the relationship or prospective relationship with a given third party.

210. Third-party due diligence enables the company to appraise individual situations, which the risk map (or even the third party's risk map) cannot do. A third party in a category classified as low risk by the risk map may be reclassified as a high-risk third party following its individual due diligence. Likewise, an incident, whistleblowing report or conviction concerning a third party in a category classified as low risk or whose behaviour changes in the course of a relationship may lead the company to perform more in-depth due diligence or to conduct due diligence as a matter of priority.

211. It could be helpful to compile an internal database of third parties in compliance with regulations. The database must be secure and up to date, which implies adopting formalised, secure procedures to create, approve, amend and delete third parties recorded in the database in strict accordance with assigned tasks and access privileges.

- **Third-party due diligence in practice**

212. Three levels of players take part in due diligence:

- Staff responsible for due diligence collect the information and documents useful for due diligence on the third parties with which the company has a relationship or a prospective relationship. They issue a first appraisal. This appraisal counts as a decision in cases judged to be low risk;
- The staff member or department in charge of the anti-corruption programme (or any other designated individual or department) provides expertise and advice to the staff in charge of due diligence and assists the operational staff with appraisals of and decisions on high-risk cases;
- Senior management decides on further action to be taken with respect to the highest-risk cases referred to it by the departments concerned.

213. As needed, the company may call on external service providers, especially when it is unable to obtain the necessary information or documents on its own, or when the third party is resident or does business in a country where the company has no presence. Under the terms of the Act, the company is liable for the quality and appropriateness of the due diligence conducted on its behalf.

214. The third-party due diligence procedure is formalised.

215. The company ascertains the information and documents useful for due diligence on the basis of its risk map.

216. As a guideline, due diligence can include:

- Collection of information by consulting the company's internal lists;
- Collection of open-source information, public documents and documents available to the public (e.g. press articles, financial statements, court rulings where published);
- A check to see whether the third party and its beneficial owners, such as they are defined by articles R. 561-1 and R. 561-2 of the Monetary and Financial Code, and its management or administrators appear on lists of sanctioned natural and legal persons (in particular, lists of persons debarred from public contracts funded by the World Bank and development banks, and the economic and finance ministries' list of persons subject to financial and international sanctions);
- Collection of information from databases sold by specialised service providers;
- Collection of information and documents from the third party by such means as a questionnaire, interview, audit and in-house approval or certification process.

217. The company notes the main elements that identify the third party: name, corporate name, the structure's legal status, date of establishment, number of employees, turnover, capital, activity sector(s), specialisation(s) (for service providers in particular) and geographic location.

218. The company ascertains the first and last names of the leading shareholders as well as those of the beneficial owners.

219. The company assesses the sensitivity of the third party's activity sector to corruption risk. For this purpose, the company may rely on its corruption risk map, as well as its business experience. It may supplement this with external analysis by international companies and non-governmental organisations.

220. The company ensures that the third party, especially in the case of an intermediary or a supplier, has the necessary experience, credentials and competence to perform its tasks. For this purpose, it may ask the third party to provide it with the professional references it deems necessary based on the data already collected (date of establishment, date of launch of the activity, etc.). A lack of credentials or experience may be defined as an aggravating factor in the assessment of the third party's risk level.

221. The company shall enquire whether the third party, its senior managers, its leading shareholders and its beneficial owners have ever been mentioned in negative reports, allegations, proceedings or convictions related to corruption (or for the offenses of concealment or money laundering related to corruption).

222. The information is obtained in accordance with the applicable regulations, especially those governing personal data protection.

223. The company could also ensure that the third party has deployed an anti-corruption programme. Where a third party says nothing about the implementation of such a programme when bound to do so by law and does not provide any documentation about it, this may be considered as a cause for vigilance.

224. Dealings between the public and private sectors give rise to an identified corruption risk. It is appropriate for the company to identify the dealings that the third party may have with public officials, especially in the case of politically exposed persons, as defined in Article L. 561-10 of the Monetary and Financial Code.

- **Assessment of the third party's risk level**

225. The company assesses the third party's risk level based on the collected information and documents and an analysis of the terms of the prospective relationship (or an analysis of the nature and purpose of the relationship). It also considers aggravating factors, such as country risk or the third party's conduct.

226. Some relationships entail acute corruption risks, as in the case of a third party given the task of helping the company to win contracts. Either the company may encourage the third party to engage in non-compliant practices to circumvent its anti-corruption programme, or the third party may engage in such practices on its own initiative, without informing the company.

227. The establishment of a long-term, high-value financial relationship may be considered a risk factor in the assessment of the third party's risk level. Furthermore, the use of certain foreign currencies is also a factor to consider, given the extraterritorial reach of some anti-corruption legislation. Likewise, the company's level of economic dependence on the third party or the third party's level of economic dependence on the company could constitute a risk.

228. The company checks that the compensation amount is consistent with the nature and volume of the goods or services sold by the third party and in line with market prices. An inconsistency could be a warning signal and the reasons for it would need to be justified.

229. The company ensures that the use of the third party is warranted and that the services provided are real, especially in the case of service providers and intermediaries.

230. The company specifies the reasons for choosing one third party rather than one of its competitors. The fact that a customer recommends or requires the use of a given third-party is a danger signal, for example.

231. The payment of commissions for winning contracts represents a risk factor in the assessment of the third party's risk level.

232. The location of third parties' bank accounts may be an aggravating factor to be considered when assessing the level of third-party risk (e.g. a bank account in an uncooperative jurisdiction).

233. In addition, some payment methods, including payments in cash, cross-border payments and payments upon presentation of unitemised invoices may constitute risk factors when assessing the third party's risk level.

234. If the third party is not located in France or if the service is rendered in another country, the assessment considers the corruption risk level of that country on the basis of:

- The list of countries subject to financial and international sanctions published by economy and finance ministries;
- Monitoring reports on the implementation of the OECD Convention on Combatting Bribery of Foreign Public Officials in International Business Transactions in the signatory countries;
- Investigations and indices on public sector corruption;
- Incorporation of the third party in an uncooperative jurisdiction or a country without equivalent legislation, which may be defined as a risk factor when assessing the third party's risk level.

235. The risk assessment considers the third party's conduct: for example, where a third party refuses to provide or delays providing requested information and/or documents, the assessment could consider this to be a risk factor.

236. The company may do business in an ecosystem made up of several players, without actually having links to every one of them (e.g. contractual chains). In this case, it may be in the company's interest to ensure that the third parties it is dealing with conduct their own third-party due diligence in accordance with the paragraphs above.

- **Conclusions to be drawn from third-party due diligence**

237. The decision-makers should be designated according to the stage of the business relationship (starting new relationship or renewing an existing relationship, etc.), the category of the third party and the third party's risk level.

238. Following the assessment of the risk level, it may be decided to:

- Approve the relationship – with or without enhanced due diligence measures;
- Terminate or refrain from proceeding with the relationship;
- Postpone the decision (pending further assessments, for example).

239. The company's decision-makers and decision-making procedures are clearly identified.

240. The absence of risk factors following an assessment does not guarantee that the relationship with the third party is absolutely devoid of risk. Conversely, the identification of risk factors does not rule out the relationship, but must lead the company to exercise appropriate due diligence during the relationship.

- **Due diligence in ongoing business relationships**

241. Corruption prevention and detection measures must be adapted to each company's environment. This means that it is up to the company to define the measures it deems to be consistent with its business model.

242. In this regard, the public sector entity may usefully envisage one or more of the following options:

- Inform the third party of the existence of its anti-corruption programme by communicating the code of conduct, for example;
- Train or raise the awareness of the third party about corruption risk;
- Require a written anti-corruption commitment from the third party or insert a clause enabling the company to terminate the contractual relationship in the event of corruption if the legal nature of the relationship with the third party so permits;
- Encourage the third party to verify the honesty of its own subcontractors to ensure the security of the contractual chain.

- **Monitoring the contractual relationship**

243. The contractual relationship needs to be clearly established in order to monitor proper execution.

244. For this purpose, the company needs complete transparency regarding payments to and from third parties to ensure that the compensation and payment methods comply with the provisions of the contract. The finance and accounting staff alert the compliance officer or any other designated person when unusual payment methods are demanded, such as cash payments, payments to a third party or to a new bank account in an uncooperative or embargoed jurisdiction.

- **Renewing and updating third-party due diligence**

245. The due diligence process is repeated at regular intervals in accordance with the third party's category and level of risk. In this respect, it is useful to set a review date when entering into a relationship.

246. Where information on a third party's situation does not affect the company's risk level, the information on the third party is updated. However, if this information reveals a significant change in the third party's situation, such as a change of beneficial owner, a merger of two entities or the acquisition of a new entity, then new third-party due diligence is undertaken.

247. The review process is the occasion to ensure that the third party has respected its anti-corruption commitments throughout the relationship.

- **Monitoring third-party due diligence**

248. Monitoring of third-party due diligence is instituted and may include:

- Indicators related to due diligence conducted;
- Review indicators tracking compliance with third-party due diligence review frequency;
- The findings of first- and second-line-of-defence controls;
- Indicators for priority reviews under an ad hoc plan for due diligence initiated following instances of non-compliance found by first- and second-line-of-defence controls.

249. Depending on their purpose, all of these indicators and findings may be submitted to superiors and to the compliance officer or any other designated person.

- **Filing information on third parties**

250. The entire third-party due diligence file and the record of changes must be kept on file for five years from the date of the end of the business relationship (or from the date of an occasional transaction), save in the case of stricter legislation.

B- Detection

1. Internal whistleblowing system

251. Under the terms of Article 17(II, 2) of the Act, the company is required to implement "*an internal whistleblowing system for receiving reports from staff about instances of conduct or situations that violate the company's code of conduct*".

- **Definition and objectives**

252. The internal whistleblowing system is the procedure that companies implement to enable their staff to inform a dedicated contact person about conduct or situations that could be code of conduct violations so that they can be eliminated and the appropriate sanctions applied, where necessary (see Appendix 1).

- **Coordination of different whistleblowing systems**

253. Various workplace whistleblowing systems, as provided for by specific laws and regulations, exist side by side. For the sake of transparency, a single technical platform for receiving whistleblower reports should be set up to ensure proper processing of the reports.

254. Setting up a single technical platform for receiving reports means that, in addition to the company's staff, external collaborators and casual workers[3] can make reports.

255. Reports on corruption that reveal shortcomings in the compliance programme may be sent to AFA.

- **Organisation of the whistleblowing system**

256. The internal whistleblowing system must be appropriate for the company's risk profile. The internal whistleblowing system specifies the role of the superior, who must be able to guide and advise staff, except where the superior is the perpetrator of the reported conduct.

258. The company ensures that the persons responsible for processing whistleblower reports are trained to respect the confidentiality of the reports they process and to manage any conflicts of interest. It also ensures that supervisory personnel are trained.

259. The internal whistleblowing system is presented immediately to new hires.

260. Management of the system, including the contact person function defined below, may be contracted out to a third party, provided the latter has the necessary competence for proper processing of whistleblower reports and the means to ensure confidentiality. The services provided for this purpose must be monitored regularly. The company ensures that the third party chosen has the resources to process whistleblower reports and makes sure that the third party's access to the relevant departments in the company is facilitated.

261. The whistleblowing system is deployed across all of the entities under the company's control.

[3] External collaborators and casual workers include temporary staff, interns, service providers and subcontractors' employees.

- **Processing whistleblower reports**

262. The internal whistleblowing procedure must specify the different steps to be followed when making a report, the procedures for the recipient's processing of the report, the rights of the persons concerned (and more particularly the protection of their rights), and the security and protection measures for personal data.

263. The internal whistleblowing system identifies:

- The contact person designated to receive reports within the company and, the person responsible for processing reports, if it is not the same person;
- The measures taken to ensure the confidentiality of the whistleblowers' identity, the reports, and the incidents reported and the persons named in the reports, even when investigation and processing of reports require communication with third parties. Breaches of confidentiality must be liable to disciplinary sanctions.

264. The whistleblowing system is secure and access privileges are restricted to personnel authorised to receive and process the reports.

265. If one or more persons is implicated, the company must take care about gathering evidence and documents, particularly when the persons named in the report are able to destroy incriminating data or documents.

266. The internal whistleblowing system specifies the procedures for access to the system and exchanging information with the whistleblower, more specifically:

- The channels for making reports: it could be a dedicated e-mail address, management software, or even, for some companies, a specific ethics platform. The report can also be submitted through the whistleblower's superiors. In all events, these channels must be easily accessible;
- Procedures for whistleblowers to provide information and documents to back up their reports;
- The business information and documents submitted by the whistleblower that may be used for an internal investigation;
- The provisions made to notify the whistleblower immediately of reception of the report and of the time needed to determine its admissibility. It should be stated that the acknowledgement of receipt does not mean the report is admissible.
- The provisions made to notify the whistleblower, and, where necessary, the persons named in the report, that the procedure is closed.

267. If automated report processing is introduced, the procedure must indicate the provisions that ensure compliance with the terms of the Data Protection Act 78-17 of 6 January 1978 and other personal data protection provisions. Personal data means any information about a natural person who is identified or identifiable.

268. In the face of growing numbers of requirements with regard to receiving reports, the French Data Protection Authority (CNIL) published its ruling 2019-139 dated 18 July 2019 setting standards for handling personal data for the purpose of implementing a whistleblowing system.

269. Reports may be submitted anonymously. The system must make it possible to continue dialoguing with the whistleblower while still maintaining their anonymity (for example, whistleblowers could be asked to provide an anonymous email address or a post office box address).

270. It is essential to define and formalise the internal investigation procedure before the system is launched, while being vigilant about the choice of investigation participants and the conduct of investigations. The investigation procedure may specify:

- The criteria for initiating an investigation;
- The procedures for conducting an investigation.

271. The persons responsible for conducting the investigation must be bound by very strict confidentiality obligations, which need to be formalised.

272. If the investigation is outsourced, the services rendered by the selected provider must be monitored regularly for compliance with the confidentiality and data protection rules.

273. Every internal investigation is conducted by one or more qualified persons to be designated by the company's senior management.

274. At minimum, senior management is kept informed about investigations opened into the most sensitive situations, with the exception of situations where senior management itself is implicated.

275. After the internal investigation, an official investigation report is drafted to present all of the facts and evidence gathered to substantiate or discredit suspicions, and to describe the method used. The internal investigation report draws conclusions about any further action needed on the whistleblower's report.

276. If the suspicions seem to be substantiated, the report is submitted to senior management (or the supervisory body if senior management is implicated) for further action.

277. If the internal investigation proves conduct contrary to the anti-corruption code of conduct, the disciplinary sanctions provided for such cases must be imposed, as decided by senior management or its delegate.

278. Legal proceedings may also be instigated against the natural person implicated, if the company decides to notify the judicial authorities by means of a complaint or a report. This notification is mandatory if the company is subject to the authorities listed in Article 40 of the Code of Criminal Procedure.

279. The reports must be used to update the risk map, while maintaining the confidentiality ensured by the system, and to draw conclusions with regard to improvements to be made to elements of the corruption prevention and detection programme (training programme, code of conduct, third-party due diligence).

- **Implementation of the internal whistleblowing system**

280. The following steps can be helpful:

- Establishing a formalised procedure that may include the appointment of a whistleblower contact and the creation of a committee of qualified persons bound by enhanced confidentiality obligations. The committee decides collectively any further action to be taken on whistleblower reports;
- Presenting the whistleblowing system in the code of conduct with reference to the said procedure;
- Disseminating the internal whistleblowing procedure to all staff by all means (letter from senior management, posters, intranet site, handouts, etc.) to ensure that everyone concerned knows about the system and has access to it. If the anti-corruption whistleblowing system is part of a joint system covering other legal requirements, the procedure must also be disseminated to the company's occasional collaborators. The company may decide to make its whistleblowing

system accessible to third parties. The company may choose to use its external communication tools, such as websites and documents provided to third parties, to talk about its whistleblowing system;

- Presenting the whistleblowing system to all staff as part of its awareness-raising actions;
- Training the staff tasked with receiving, managing and processing whistleblower reports, with particular emphasis on confidentiality obligations and training the staff with the greatest exposure;
- Establishing first- and second-line-of-defence controls of the internal whistleblowing system and incorporating this system (and all of the other tools in the corruption prevention programme) into the internal audit plan as part of the third line of defence. The three lines of defence mentioned above may be adapted to avoid any conflicts of interest or self-auditing. When necessary, it is important for the staff processing a whistleblower report to be different from the staff who audit report processing and for an ex-post audit to be conducted;
- Implementing indicators to assess the quality and effectiveness of the whistleblowing system (including the number of reports received, shelved or processed, processing times, problems raised). These indicators are submitted to senior management.

- **Archiving whistleblower reports and their follow-up**

281. The retention and archiving periods for personal data relating to whistleblower reports differ depending on whether further action is taken.

282. If the processing manager decides to take further action[4] on a whistleblower report, or if disciplinary action or litigation is initiated, all of the personal data collected during the investigation may be retained until the end of the proceedings, up to the statute of limitations (six years), or until after all appeals have been exhausted.

283. If the investigation of a whistleblower report does not lead to any further action, personal data must be destroyed or rendered anonymous within two months of closing the investigation.

284. When whistleblower reports are received through a single technical platform and they do not relate to conduct that could be qualified as corruption, the retention periods are determined by Decree 2017-564 of 19 April 2017 on the procedures for receiving whistleblower reports within public sector entities, private sector entities and central government administrations.

2. Internal control

- **Contribution of the internal control and audit system to the prevention and detection of corruption risks**

[4] "Further action" means any decision made by the organisation to act on the whistleblower report. This may involve new or amended internal rules (rules of procedure, ethics charter, etc.), reorganisation of the company's operations and departments, sanctions or legal proceedings (see the CNIL practical guide on retention periods).

285. Article 17 of the Act requires the companies subject to its provisions to establish accounting control procedures and an internal control and assessment system for the measures that make up its anti-corruption programme.

286. Companies usually have a general-purpose internal control and audit system with up to three lines of defence:

- The purpose of the first line of defence[5] is to ensure that the tasks that are part of an operational or support process are performed in compliance with the company's procedures. These controls may be performed by the operational or support staff or by their superior;
- The purpose of the second line of defence[6] is to ensure that the first-line-of-defence controls are properly executed. These controls may be conducted at prescribed intervals or randomly. Second-line-of-defence controls are performed by the compliance officer, the quality function, the risk management function or management control;
- The purpose of the third line of defence, also known as "internal audit", is to ensure that the control system complies with the company's requirements and is implemented effectively and kept up to date.

287. In addition to implementing the requirements set out in Article 17 of the Act, this general-purpose internal control and audit system may also be helpful for ensuring broader coverage of the company's risks identified in the corruption risk mapping exercise.

288. The company can use the risk map to:

- Identify high-risk situations that are not covered or poorly covered by control measures;
- Assess existing control measures that could manage these risks.

289. Therefore, the company is encouraged to ensure that its general-purpose internal control and audit system:

- Covers the high-risk situations identified by its corruption risk mapping exercise,
- Is appropriate for these risks and capable of managing them;
- Is updated regularly on the basis of the risks encountered and the findings of the controls conducted.

290. The controls defined in this way supplement the action plan derived from the corruption risk mapping exercise.

291. The controls defined in this way are formalised under a procedure that specifies the identified high-risk processes and situations, the frequency of controls and control procedures, the persons responsible for controls and the procedures for submitting their findings to senior management.

- **Accounting controls**

292. Of the internal control and audit procedures, accounting control and audit procedures, which help manage companies' risks, are one of the preferred tools for preventing and detecting corruption.

[5] This control and audit activity is preventive and is conducted before a decision or transaction is implemented.
[6] This control and audit activity is detective and is conducted on all or some of the decisions or transactions implemented.

293. A company's accounts are an assessment tool that provide information about its activity and its intangible, tangible and financial assets. Accounting entries are made, classified, restated and aggregated to produce statements that faithfully represent transaction details.

- Definition and objectives

294. The purpose of the accounting controls stipulated in Article 17 of the Act (hereinafter "anti-corruption accounting controls") is to "*ensure that the books, ledgers and accounts are not used to conceal bribery or influence trafficking*".

- Coordination with existing accounting controls

295. Companies have general-purpose accounting control procedures to provide reasonable assurance about the quality of accounting information. These procedures ensure the regularity, accuracy and reliability of the accounts and financial statements.

296. Anti-corruption accounting controls:

- Ultimately ensure compliance with the same principles as general-purpose accounting controls (lawfulness, accuracy and reliability of accounts and financial statements);
- Seek, more specifically to detect unwarranted and unjustifiable transactions, such as inadequately explained payments into "slush funds";
- Use the same methods as general-purpose accounting controls, including sampling, consistency reviews, physical controls (inventory counts) and third-party confirmations.

297. The procedures are instituted by enhancing or supplementing existing general-purpose controls with regard to the high-risk situations identified by the corruption risk mapping exercise.

298. Examples of high-risk situations to be addressed in this manner, if they are identified by the risk mapping exercise, may include:

- Transactions such as sponsorship, patronage, fees and commissions, travel and entertainment expenses, gifts and hospitality, donations, legacies, etc.;
- Unusual transactions (e.g. suspense accounts and temporary accounts);
- Extraordinary and high-stakes transactions;
- Transactions involving third-parties from high-risk groups, such as intermediaries or consultants;
- Movements or funds or commodities to and from accounts or third parties belonging to a high-risk group, such as intermediaries or commercial agents;
- Off-balance sheet commitments, such as:
    - Commitments made on behalf of third parties (e.g. executives, subsidiaries),
    - Collateral,
    - Guaranties.

299. The risk mapping exercise may also reveal that management of some account items is a high-risk process, as in the case of reversing entries, discounts and rebates, sundry expenditures and cash floats. Balance sheet items may also involve a high level of risk, such as goodwill or suspense accounts and imprest accounts.

- Formalising anti-corruption accounting controls

300. Anti-corruption accounting control procedures are formalised under a procedure that sets out:

- The purpose and scope of controls;

- Roles and responsibilities for their implementation;
- Sampling procedures for transactions subject to controls, as appropriate;
- Definition of a control plan;
- Procedures for managing incidents;
- Threshold and materiality criteria that trigger controls.

▪ Content of anti-corruption accounting controls

301. The anti-corruption controls for the first line of defence are generally performed by the persons responsible for entering and validating accounting entries. These persons ensure that the entries are properly justified and documented (especially manual entries).

302. Companies should ensure that high-risk accounting entries are reviewed and validated by a different person than the person making the entries to mitigate the risks associated with self-auditing.

303. Reciprocal validation between staff members is satisfactory for entries involving sums under a designated threshold. Entries for greater amounts require approval from a superior.

304. The accounting anti-corruption controls for the second line of defence are performed all year long by persons who are independent from those who performed the controls for the first line of defence.

305. The purpose of these controls is to ensure proper performance of the anti-corruption accounting controls for the first line of defence. When sampling is used, the sampling method must be representative of the inherent risks in the transactions (including manual entries, approval authority and segregation of duties). The sampling procedures are defined with regard to a prior analysis of the various entries and risks concerned to ensure representativeness.

306. If the anti-corruption accounting controls for the first line of defence are automated, the controls for the second line of defence should be adapted in consequence.

307. The findings of the anti-corruption accounting controls for the second line of defence are summarised with the definition of corrective actions as part of an action plan if any problems are found.

308. The effectiveness of anti-corruption accounting controls is assessed on a regular basis as part of the accounting controls for the third line of defence, which are also called "*accounting audits*".

309. Such accounting audits cover the whole accounting system to ensure that the anti-corruption accounting controls comply with the company's requirements, and that they are effectively implemented and kept up to date.

310. For this purpose, the accounting controls for the third line of defence assess the appropriateness and effectiveness:

- Of governance and resources for anti-corruption accounting controls;
- Of the methods for the development (particularly the integration of the corruption risk map) and application of anti-corruption accounting controls for the first and second lines of defence.

▪ Treating any problems found

311. If a problem is found, certain existing accounting procedures may be amended to remedy the problem.

312. Problems found also contribute to updates of the corruption risk map and may be presented in coordination with the compliance officer as additional examples to illustrate the code of conduct and training materials on preventing corruption.

313. If the problem stems from a failure in the implementation of procedures or the anti-corruption programme, the superior may consider taking measures against the person responsible for the failure. These measures may range from a reminder about the rules to a sanction, depending on the severity of the failure.

314. If the problem leads to suspicions or cases of corruption, it must be reported to the compliance officer and senior management, which may decide to launch an internal investigation.

- Outsourcing

315. Anti-corruption accounting controls may be implemented;

- Internally, by the accounting and finance departments or by specialised functions (shared services centres, management control, internal audit, etc.) that the company calls on for this purpose;
- Externally, by entities that the company mandates for this purpose.

316. Some companies are required to appoint a statutory auditor to certify their financial statements. This auditor's actions and assigned objectives contribute to preventing potential problems for the audited company and to preventing and detecting corruption. The auditor is required to notify the public prosecutor of any presumed offences, including corruption, found when conducting the audit.

C – Monitoring and evaluation of the anti-corruption programme

1. Purposes and procedures

317. The company develops an internal control monitoring and evaluation system to ensure that the measures and procedures stipulated in Article 17 of the Act are appropriate and effective. This system may be incorporated into the general-purpose internal control and audit system.

318. This system meets four objectives:

- Monitoring implementation of anti-corruption programme measures and testing their effectiveness;
- Identifying and understanding any deficiencies in the implementation of the procedures;
- Formulating, where necessary, recommendations or other appropriate corrective measures to improve the effectiveness of the anti-corruption programme;
- Detecting any corruption.

319. Monitoring may be structured around the three lines of defence mentioned above.

320. The compliance officer drafts a monitoring plan for the second line of defence to cover the entire anti-corruption programme.

321. The plan specifies the purpose and scope of each monitoring activity, along with the persons responsible, the methods (types of measurements, documentation, analysis and evaluation), and, where appropriate, the sampling procedures based on risk analysis. The plan also specifies the frequency of monitoring, formalisation, communication of findings and corrective measures that could be implemented, along with record retention procedures.

322. Deficiencies identified by monitoring of the second line of defence are written up in a report approved by the compliance officer. It can be helpful to submit a summary of the report to senior management and to the internal audit function.

323. The adequacy and effectiveness of the anti-corruption programme's measures and procedures are regularly evaluated by monitoring by the third line of defence or internal audit. The purpose of these internal audits is to ensure that the anti-corruption programme complies with the company's requirements, is implemented effectively and is kept up to date. The internal audit function is also encouraged to ensure that the high-risk situations identified by the corruption risk map are covered by effective preventive measures.

324. These audits are formalised, documented and retained. A substantiated and documented audit report sets out the corrective measures and recommendations. This report is submitted to senior management.

2. Typology of monitoring

325. Monitoring is defined and implemented for the first, second and third lines of defence for each measure and procedure mentioned in Article 17 of the Act.

326. AFA recommends that this monitoring focus on the following elements:

	327 **Corruption risk map**
First line of defence **Second line of defence**	Monitoring linked to the risk map cannot be performed until the map is produced and after each update. No first-line-of-defence monitoring can be performed in this case. Furthermore, the function that is responsible for overseeing the anti-corruption programme and took part in the risk mapping exercise or updates cannot perform second-line-of-defence monitoring of its own work.
Third line of defence	- Review of the scope of the map, the methodology used and the deployment of the associated action plans; - Analysis of the deficiencies found and incidents (with a view to updating the map); - Analysis of governance and proper allocation of resources. Analysis of the systematic nature of the programme. - Analysis of the illustrations provided in the code of conduct with regard to the risks identified by the risk map; - Analysis of the targeting and content of training with regard to the risks identified by the risk map; - Analysis of incidents reported by whistleblowers or found by accounting audits, and the consequences for updating the map; - Analysis of the adequacy of third-party due diligence with regard to the risks identified by the map
	328. **Code of conduct.**
First line of defence	- Approval of transactions or situations governed by the policies and procedures contained in or appended to the code of conduct (particularly on gifts and hospitality).
Second line of defence	- Periodic monitoring on the correct performance of first-line-of-defence controls; - Sampling to monitor compliance with the policies and procedures contained in or appended to the code of conduct. *E.g. definition of a quarterly sample of XX expense claims based on risk analysis. Then analysis the consistency of the voucher with the claim, the names of the guests, compliance with thresholds and approvals.* - Review of the content of the code with regard to legal requirements and the risk map, and the incorporation of the code of conduct into the rules of procedure of the entities concerned. - Ensuring that the illustrations provided in the code of conduct are still appropriate after each update of the risk map.

Third line of defence	- Audit of proper execution and effectiveness of the first- and second-line-of-defence monitoring. - Analysis of the communication, dissemination and accessibility of the code of conduct and the policies and procedures contain in it or appended to it. - Analysis of the systematic nature of the programme. *E.g. a critical analysis of the content (particularly the illustrations) of the code of conduct with regard to the scenarios identified by the map and the incorporation of the code of conduct content into the training programme*
	329. **Training**
First line of defence	- Verifying the attendance of the employees concerned and the knowledge acquired during training. r
Second line of defence	- Periodic monitoring of the correct performance of first-line-of-defence monitoring; - Ensuring that training content is appropriate for target audiences and their risk exposure as identified by the map. - Review the attendance of the staff concerned and potential sanctions for failure to attend training sessions.
Third line of defence	- Monitoring proper execution and effectiveness of the first- and second-line-of-defence controls. - Analysis of governance and proper allocation of resources. *For example, analysis of procedures (in-person/remote learning, etc.) and training content for managers and staff with the greatest exposure to specific risks*. - Analysis of the systematic nature of the programme. *E.g. analysis of the targeting and content of training for managers and the staff with the greatest exposure to the risks identified by the map. Ensure references to the code of conduct and whistleblowing system are clear.*
	330 **Third-party due diligence**
First line of defence	- Monitoring the application of the third-party due diligence procedures. *E.g. before entering a relationship with a new supplier, verify:* • *That all of the documents required for the procedure (e.g. list of beneficial owners, answers to a questionnaire, etc.) have been gathered;* • *That the necessary research has been conducted (open sources, databases, etc.);* • *That the assessment is consistent with the evidence analysed;* • *That the decision to accept or reject the new relationship has been properly formalised*.

Second line of defence	- Regular monitoring of the proper execution of the first-line-of-defence monitoring, based on a representative sampling; - Verification of the implementation of due diligence measures and effective monitoring of them; - Verification of due diligence updates (periodic reviews of assessments or after a whistleblower report); - Monitoring the appropriateness of the due diligence measures deployed.
Third line of defence	- Audit of proper execution and effectiveness of the first- and second-line-of-defence monitoring. Analysis of the systematic nature of the programme. *E.g. Audit of the adequacy of third-party due diligence with regard to the risks identified by the map.* *Ensure that accounting control systems are updated with regard to the risks identified by third-party due diligence*.
	331. **Internal whistleblowing system**
First line of defence	- Monitoring the deployment and correct use of the whistleblowing procedure; *E.g. monitor the accessibility to the whistleblowing channels and broad-based communication about the whistleblowing system, acknowledgements of receipt and examination of the admissibility of the whistleblower reports, identification of the roles and responsibilities of the investigation team, closing investigations, notification of closed investigations, sanctions and action plans, maintaining confidentiality and anonymity, monitoring protection measures.*
Second line of defence	- Regular monitoring of the proper execution of the first-line-of-defence monitoring, based on a representative sampling;
Third line of defence	- Audit of proper execution and effectiveness of the first- and second-line-of-defence monitoring. - Qualitative and quantitative analysis of the whistleblower reports received over the period (the channels used, reports submitted through other unidentified channels, issues raised in the reports). - Audit the adequacy of the responses to the reports received. Analysis of the systematic nature of the programme. *E.g. consideration of whistleblower reports when updating the risk map, third-party due diligence and accounting controls. Verify that employees are trained or informed about the whistleblowing system and that the persons responsible for processing whistleblower reports receive special training.*
	332. **Accounting controls.**
First line of defence	- Automated monitoring of certain transactions; - Monitoring approval authority;

	- "Four eyes rule": review by an employee other than the one recording the transaction; - Monitoring the proper application of anti-corruption accounting monitoring before the transaction is executed.
Second line of defence	- Regular monitoring of the proper execution of the first-line-of-defence monitoring after transactions are executed and based on a representative sampling;
Third line of defence	- Audit of proper execution and effectiveness of the first- and second-line-of-defence monitoring. - Analysis of the execution of accounting controls and the proper allocation of resources; - Analysis of the appropriateness of the accounting controls with regard to the risks identified by the map. Analysis of the systematic nature of the programme. *E.g. Critical analysis of existing accounting control measures with regard to updates of the corruption risk map.*
	333. **Disciplinary rules**
First line of defence	The compliance of the disciplinary rules cannot be monitored until sanctions are imposed.
Second line of defence	- Monitoring sanctions imposed for each incident; - Verification that the sanction is appropriate for the incident.
Third line of defence	- Audit of proper execution and effectiveness of the first- and second-line-of-defence monitoring. Analysis of the systematic nature of the programme. *E.g. Analysis of the sanctions imposed and the need to enhance senior management's communication or for further training about a specific measure under the anti-corruption programme*.

334. If a company's anti-corruption programme includes other measures and procedures, in addition to those stipulated in Article 17 of the Act, AFA recommends that these measures and procedures should also be covered by the internal monitoring and evaluation systems instituted.

335. First-line-of-defence monitoring is formalised and documented.

336. A formalised monitoring plan is drawn up for the second line of defence monitoring describing the scope, roles and responsibilities, frequency, sampling procedures, formalisation specifications, further action on irregularities and the associated action plans.

337. A formalised audit programme is drawn up for the third line of defence describing the scope, sampling procedures, formalisation specifications, further action on irregularities found and the associated action plans.

D- Corrective action

1. Management and follow-up of deficiencies found

338. Deficiencies associated with the implementation of procedures – and potentially reported by the monitoring and audits – are analysed to identify their cause and remedy them.

2. Disciplinary system

- **Definition**

339. The disciplinary system is made up of all of the measures that a company reserves the right to impose for what it deems to be misconduct.

340. Misconduct that can warrant sanctions includes failure to comply with the disciplinary rules set out in the rules of procedure and the anti-corruption code of conduct that has been incorporated in them. Companies with 20 or more employees are required to have rules of procedure. Sanctions cannot be imposed on staff members unless the sanctions are stipulated in the rules of procedure.

- **Principle of a scale of sanctions**

341. The disciplinary sanction must be proportionate to the misconduct, as set out in the scale of sanctions stipulated in the disciplinary rules.

- **Mechanism**

342. When staff members are found to have failed to fulfil their duties of integrity and honesty, a disciplinary procedure is initiated against them and proportionate sanctions are imposed on them.

343. Senior management is not bound to wait for a criminal court's ruling before imposing disciplinary sanctions, if the misconduct is proven and serious enough to warrant sanctions. Disciplinary sanctions may be imposed on the basis of the findings of a detailed internal investigation that firmly establish the materiality of the accused person's misconduct.

- **Sanctions report**

344. A report of disciplinary sanctions imposed on the entity's staff helps strengthen corruption risk management mechanisms.

345. Irrespective of the medium used for this report, the company ensures the strict confidentiality of its content and compiles it in accordance with the personal data protection rules.

- **Internal communication**

345 b. Senior management may request the dissemination of disciplinary sanctions report, in a way that guarantees total anonymity, to highlight its policy of zero tolerance for any corruption or misconduct.

III. Adaptation of the general provisions to public sector entities subject to Article 3(3) of the Act

346. The following provisions adapt and specify the provisions set out in paragraphs 13 to 84 of these guidelines for public sector entities subject to Article 3(3) of the Act.

347. The Act gives the French Anti-Corruption Agency jurisdiction to audit, "*the quality and effectiveness of the procedures implemented by central and local government administrations, their public establishments and semi-public companies, and recognised public-interest non-profits to prevent and detect bribery, influence peddling, extortion by public officials, unlawful taking of interest, misappropriation of public funds and favouritism*." The law establishes the requirement for entities so defined (hereafter "public sector entities") to deploy an anti-corruption programme.

348. The purpose of these guidelines is to facilitate the accomplishment by public sector entities of the objectives defined by the Act by proposing implementation procedures for an anti-corruption programme.

349. The particularity of public sector entities in terms of preventing and detecting corruption resides in their wide range of tasks, responsibilities, legal forms, governance structures, geographic coverage, governing standards of integrity, staff statuses, categories of third parties with which they interact and size. Public sector entities are consequently asked to implement the guidelines in a manner proportionate to their risk profile. They may equally use other methods to achieve the same results.

350. The legal regimes applicable to the different categories of public sector entity are too many and varied for these guidelines to detail all the mandatory provisions that apply to public sector entities and play a part in the prevention and detection of corruption. Nevertheless, these guidelines do focus on particular points that concern a large number of public sector entities.

351. Public sector entities with control over other entities (e.g. foundations, subsidiaries, local publicly-owned companies, public establishments, etc.) ensure the quality and effectiveness of the anti-corruption programme(s) deployed in all the entities they control. In this regard, they may choose either to develop their own anti-corruption programme for the entities they control (e.g. for small entities) or to put in place procedures and internal controls to ensure the quality and effectiveness of the anti-corruption programme(s) deployed in all the entities they control.

352. The public sector entitiy's anti-corruption programme concerns, in addition to the staff, the members of senior management, all elected officials who are not members of senior management and ministers' private office staff as well as, where applicable, volunteers involved in its activities.

III.1) First pillar: senior management's commitment

353. The requirements for public sector entities to put in place procedures to prevent and detect corruption derive not only from the Act,[7] but also for the most part from different legislative and regulatory provisions. For public sector entities employing public servants, these are mainly ethical requirements (disclosure of interests and assets by certain elected officials and senior executives, recusal or abstention in the event of a conflict of interest, regulation of multiple jobholding, prevention of conflicts of interest when a public servant leaves the civil service, requirement to appoint a compliance officer, etc.).[8] Other provisions also have a role to play in reducing the risks of corruption such as the General Local Government Code provisions governing the holding of deliberative assemblies, the public procurement

[7] Articles 3 & 8 of the Act and Decree 2017-564 of 20 April 2017 on reception procedures for whistleblowing reports in government and business entities, or in central government departments.

[8] In particular, the Transparency in Public Life Act 2013-907 of 11 October 2013, the Civil Servants' Rights and Obligations Act 83-634 of 13 July 1983 amended by the Civil Servant Ethics and Rights and Obligations Act 2016-483 of 20 April 2016; the Civil Service Transformation Act 2019-828 of 6 August 2019; and the Ethics Audits in the Civil Service Decree 2020-69 of 30 January 2020.

rules and the amended Public Accounting and Budget Management Decree 2012-1246 of 7 November 2012.

354. The onus is therefore on senior management to ensure that the persons concerned are aware of and implement these provisions. Failure to do so could incur senior management's administrative or criminal liability.

355. Nevertheless, the implementation of these legislative and regulatory provisions does not in itself constitute a comprehensive, effective corruption prevention and detection programme. These guidelines are therefore designed to help public sector entities develop such a programme.

1. Definition of senior management

356. Senior management consists of those persons – elected or appointed – with the authority and powers to manage a public sector entity, pursuant to its articles of association and the legislation and regulations in force.

357. This definition includes the following persons and bodies:

- For central government departments: minister, secretary-general, central administration director, prefecture authority and devolved department manager;
- For local and regional government bodies: executive body (mayor and president of the *département* council, regional council, local council, assembly, etc.), chair of the public establishment for intermunicipal cooperation (EPCI) and general manager;
- For public establishments and semi-public companies: chair of the board of directors and director;
- For state-funded healthcare institutions: director;
- For recognised public-interest foundations, depending on their chosen organisation: chair of the supervisory board, chair of the management board, chair of the board of directors and director;
- For recognised public-interest associations: chair and director.

358. These persons and bodies are empowered to organise the entity or department, allocate resources and represent the entity, which gives them a decisive role to play in setting up an anti-corruption programme.

2. Senior management's responsibility

359. Senior management commits to a policy of zero tolerance for any conduct that could constitute corruption and promotes and disseminates the culture of integrity within the public sector entity and vis-à-vis third parties by making corruption prevention and detection a priority.

360. Senior management is responsible for setting up the anti-corruption programme. Senior management may, where appropriate and retaining its personal responsibility, delegate the operational implementation and management of the anti-corruption programme to a staff member or department.

361. Whichever type of organisation is chosen, delegates must have a hierarchical position that guarantees the independence and legitimacy required to perform their role. This position should facilitate direct access to senior management.

362. Senior management defines the risk management strategy and ensures that the anti-corruption programme is implemented and effective. In this respect, it is responsible for formally approving the programme and, in particular, the corruption risk map. It ensures that a related action plan is developed and suitable resources provided to conduct and regularly monitor it.

363. Senior management ensures that compliance with the corruption prevention and detection measures is taken into consideration when setting annual goals and assessing its managers' performance. Managers' initiatives to promote the prevention and detection of corruption to their teams should be rewarded.

364. Senior management uses indicators and control and audit reports to check that the anti-corruption programme is organised, effective and up to date.

365. Implementation of the anti-corruption programme measures and procedures calls for senior management to incorporate risk management measures into its organisation's stated public policies and procedures, including human resources management, public procurement and the allocation of public subsidies.

366. Senior management imposes, with due regard to applicable standards (labour law and civil service regulations), appropriate disciplinary sanctions in the event of corrupt conduct, violation of the code of conduct or breach of the duty of integrity.

367. Senior management ensures that the entities controlled by the public sector entity (de jure or de facto) are covered by an anti-corruption programme.

368. Senior management ensures that the anti-corruption programme is applicable to senior management itself.

369. When senior management performs its duties and functions under the control or oversight of a non-executive or supervisory body, the latter ensures that corruption risks are covered by setting up a suitable, effective anti-corruption programme.

3. Dedicated resources

370. The implementation of an anti-corruption programme calls for human and financial resources proportionate to the public sector entity's risk profile.

371. The appointment of the staff member or department tasked with the operational implementation and management of the prevention and detection programme could be announced in a special memorandum to all staff and, where appropriate, formalised by a brief from senior management stating:

- The assigned tasks;
- The elements guaranteeing the appointee's independence, such as hierarchical position and procedures for access to senior management;
- Coordination with the public sector entity's other functions;
- Human and material resources allocated or available for allocation.

372. Senior management ensures that this staff member or department has the resources and competence to be able to perform their role, coordinate the relevant functions and report to senior management.

373. The staff member or department's hierarchical position in the structure must guarantee:

- Access to all useful information to gain a true and fair view of the public sector entity's activity;
- Independence of other functions and the capacity to have a real influence on these other functions;
- Ease of access to senior management to ensure voice and support.

374. Irrespective of their position in the organisation chart, the staff member or department keeps in direct, regular contact with senior management.

4. An appropriate internal and external communication policy

375. Senior management communicates its corruption prevention and detection policy and the entire programme that operationalises it to all the elected officials, staff and third parties (users, suppliers, service providers, associations and partners).

376. In-house anti-corruption programme communication adapted to the body's structure and activities necessarily covers the code of conduct and ethics, training and the internal whistleblowing system.

III.2) Second pillar: corruption risk mapping

377. Corruption risk mapping is a key tool for taking stock of corruption risks. It is used by public sector entities to engage in and formalise in-depth examination of their risks and to create the right conditions for improving their management of those risks. Risk mapping is conducted to protect against risks and their potential reputational, legal, human, economic and financial repercussions.

378. A corruption risk map may be specific or integrated into a general risk map, providing a methodology is used that offers reasonable assurance that the corruption risks identified, assessed and ranked truly reflect the public sector entity's real risk exposure.

379. The purpose of risk mapping by public sector entities is to manage the risks of all the corruption offences set out in Article 1 of the Act.

380. For public sector entities falling within the scope of both Article 3 and Article 17 of the Act (i.e. public industrial and commercial establishments and semi-public companies with turnover and numbers of employees over the thresholds set by Article 17), risk mapping must include the risks relating to all the corruption offences set out in Article 1 of the Act.

381. Corruption risk mapping calls for:

- Accurate knowledge of the public sector entity and its activities, including the processes[9] involved in these activities. This knowledge is required for the detailed process analysis, which guarantees that the corruption risk map truly reflects the public sector entity's real risk exposure. Each public sector entity produces its own risk map, which is specific to that entity and therefore cannot be transposed directly to another public sector entity.
- Identification of the roles and responsibilities of the players concerned at all levels of the organisation.

1. Purposes of corruption risk mapping

382. Corruption risk mapping gives senior management the knowledge it needs to take effective prevention and detection measures proportionate to the risks identified by the map and adapted to the activities of the public sector entity concerned.

383. As the second pillar of the prevention and detection programme, corruption risk mapping enables the public sector entity to effectively manage its risks by identifying the preventive, detective and corrective measures and procedures to be implemented. The lessons learned from the implementation of these measures and procedures are then fed back into the corruption risk map and its updates. All of these interactions are part and parcel of a systemic approach to corruption risk mapping and to the design and implementation of risk management measures and procedures.

2. Corruption risk map characteristics

384. The risk map is complete when it covers:

- All the players including elected officials, ministers, the different ministers' private office staff, public accountants, general economic and financial auditors and all staff irrespective of their status (tenured staff, contract staff, staff on assignment, staff on private-law contracts, temporary staff, apprentices, trainees and volunteers);

[9] In these guidelines, the notion of processes refers to a set of correlated or interacting tasks designed to meet a managerial, operational or support need.

- "End-to-end", the managerial, operational and support processes conducted by the public sector entity for its activities. Based as it is on an analysis of all the public sector entity's processes and identification of the corruption risks at each step of these processes, the risk map takes stock of these risks by taking into account each public sector entity's particularities: tasks, responsibilities, speciality, governance structure and decision-making channels, staff status, geographic coverage, third party typologies, own resources, etc.;
- The public sector entity's entire range of intervention, i.e. all the structures including the entities it controls. If the choice has been made for all or part of the controlled structures to conduct their own corruption risk mapping, the public sector entity r ensures that the maps do indeed exist and that suitable methods have been chosen to draw them up.

385. The corruption risk map is formalised, i.e. it takes the form of written, structured and auditable documentation. The risk map must take a form suited to its use as a risk steering tool and must facilitate internal appraisal (mainly by audit) and external appraisal (in the event of administrative supervision or legal action) of the appropriateness of the anti-corruption programme.

386. The public sector entity may choose to organise the documentation by responsibility, process, entity or geographic coverage, for example. The documentation contains an appendix describing the drafting roles and responsibilities and the procedures and methodologies used to identify, assess, rank and manage corruption risks.

387. A risk map is a dynamic document since risks need to be reviewed regularly, in particular whenever an important aspect of the public sector entity changes. This updating places mapping within a continuous improvement process used by public sector entities to enhance their risk management.

3. Corruption risk mapping steps

388. Corruption risk mapping is based on an objective, structured and documented analysis of the risks to which a public sector entity is exposed in the course of its activities. The description identifies the impact of the risks (severity) and the likelihood of occurrence (frequency), factors that may exacerbate them (aggravating factors) and the responses made by the existing risk management system or to be made by an action plan.

389. Consequently, the following steps are recommended to identify, assess and manage corruption risks, or another method that is at least as effective and appropriate may be used.

390. Public sector entities already familiar with mapping risks, such as operating, strategic, fiscal, accounting and European fund management risks, could capitalise on these pre-existing approaches providing the mapping method used complies with the following guidelines, since the method used for corruption risk mapping is similar: the public sector entity has already produced a description of all or part of its processes and has experience in identifying and rating risks as well as in defining a risk management strategy. The risk scenarios already identified for the operating, strategic, fiscal, accounting or European fund management risks can hence be examined and enriched, where appropriate, with their integral corruption risks. Nevertheless, this process does not guarantee that the risk scenarios identified in this manner truly reflect the corruption risks to which the organisation is really exposed. Use of the process analysis method presented below could usefully round out this approach.

Step 1: Roles and responsibilities of corruption risk mapping stakeholders

391. Public sector entities can usefully assign roles and responsibilities as follows:

- Senior management promotes the risk mapping exercise and provides suitable resources to the staff member or department to which it has assigned the task. It checks the reasoning behind the risk management strategy used and ensures that the chosen action plan is implemented;
- The relevant staff member or department coordinates the risk mapping, assisting the departments with process identification, identification of corruption risks, assessment and ranking of these risks, and the definition and implementation of measures to manage them. The relevant staff member or department communicates each risk map update and action plan monitoring report to senior management;
- The decision-making process, operational, accounting and support managers contribute to the development and updating of the risk map by reporting on the specific risks in their area of responsibility;
- Staff, by virtue of their practical experience of the public sector entity's processes, contribute to the mapping exercise by reporting on the factors specific to their functions and their related risks.

392. When mapping, the public sector entity ensures that it takes stock of the risks inherent in the activities conducted by all the staff working in the structure, irrespective of their status (including volunteers and trainees), as well as those associated with the duties and functions of the managers, elected officials and their staff.

Step 2: Identification of risks inherent in the public sector entity's activities (process identification and risk scenarios)

393. Identification of the public sector entity's risks entails a detailed analysis of its processes:

- In a first step, the public sector entity identifies these processes, where applicable using an already established process map. It is important in this first inventory that the public sector entity is careful not to come to a foregone conclusion regarding the findings of the risk mapping by drawing up an ex-ante list of processes deemed the most representative or most exposed to risks. If a public sector entity does not have a process library, a first step in identifying the processes could be to target the macro-processes using the methodology described in following paragraphs. This first step would need to be followed by a review at a more detailed level of the processes and associated risk scenarios.
- In a second step and based on the process identification, the public sector entity talks to staff (workshops, individual interviews, etc.) from all hierarchical levels and all public sector entity functions chosen for their operational command of these processes. These discussions allow participants to freely express their views and are written up in reports.

394. The purpose of these discussions is to identify, per process, the risk scenarios[10] to which the public sector entity is exposed in terms of its activities and certain lines of work. The aim is not to set out the theoretical typology of risks to which the public sector entity is exposed, but to take an accurate inventory that can be used to identify in detail and document the associated risk scenarios. Although these discussions could draw on a list of risks drawn up in advance, such a list cannot be allowed to pre-determine the nature,

[10] A risk scenario is a situation with the potential for corruption, such as non-disclosure of a conflict of interest by a staff member in charge of deciding whether to grant a subsidy to an association whose president is his spouse or failure to check a delivery by a staff member in charge of certifying the service rendered by a supplier.

number and classification of the risk scenarios chosen following the discussions: the public sector entity must base its mapping on the reality of its processes.

395. Risk mapping includes the interventions the public sector entity's third parties, which can present a risk of exposure to illicit solicitation (risk factor).

396. The risk scenarios are identified considering essentially the following risk factors:

- The public sector entity's internal organisation, in particular its governance;
- Its geographic organisation, including devolved administrations and central government agencies;
- Senior management and staff's "interconnected interests";
- The nature of the third parties with which the public sector entity interacts, for example in its procurement and when granting support and subsidies or issuing authorisations, as well as the third party's activity sectors, the nature of the relationship (direct or indirect), the level of economic dependence, etc.;
- Past incidents, particularly incidents affecting the public sector entity revealed by internal audits or by internal or professional conduct whistleblowing systems and incidents giving rise to disciplinary action or court rulings concerning similar public sector entities, observations from the Government Audit Office and the Regional Audit Office, and feedback from a legality audit.

Step 3: Assessment of gross risks

397. The purpose of this step is to assess the public sector entity's vulnerability to each risk scenario identified in step 2. The aim here is to identify the public sector entity's "gross" risk exposure, i.e. the risks considered before any management measures are taken.

398. This vulnerability is assessed using the following three indicators: impact, frequency and aggravating factors.

399. An analysis is conducted of the impact of each identified risk scenario. Impacts may be reputational, human, financial, economic or legal. A single risk scenario may have more than one type of impact.

400. Probability is determined using the fullest, most suitable information for the specific nature of the identified risk (e.g. past incidents).

401. Aggravating factors are assessed by applying severity coefficients. For example, in the case of public sector entities developing international activities, this coefficient captures the impact of geographic location at the gross risk assessment stage.

402. The discussions held to identify the risks can be put to good use to assess the identified gross risks. Irrespective of whether it draws on these discussions, the gross risk assessment is conducted using a uniform methodology. The public sector entity ensures that the gross risk assessments produced by its different components can be consistently aggregated.

Step 4: Assessment of net or residual risks

403. This step assesses the extent of risk management by the public sector entity in order to determine its "net" or "residual" risk exposure. This consists of re-assessing the "gross" risk scenarios after implementation of existing risk management measures.

404. The purpose at this stage of mapping is therefore to assess the effectiveness of the existing risk management measures, such as those intrinsic to the existence of formalised procedures, training measures and internal controls, based mainly on the audits conducted.

405. **N.B.** In an "integrated" risk mapping exercise, where the risk level of a scenario or process is assessed by aggregating different kinds of risk, including the corruption risk, steps need to be taken to ensure that this assessment rates the corruption risk as such.

Step 5: Net or residual risk ranking and preparation of the action plan

406. Once the "net" or "residual" risks have been assessed, a classification of risk scenarios by level emerges.

407. Where these risk scenarios return the same net assessment level, and where the public sector entity deems it useful to separate them out to prioritise the actions to be taken, they should be ranked using an objective methodology suited to the public sector entity's particular activities based on a combination of different criteria such as the allocated budget share and the nature and type of relationships with third parties.

408. The purpose is to determine, as part of the risk management strategy, the measures to be taken to manage the risks.

409. An action plan is developed on the basis of these elements. Specifically appointed players are placed in charge of the action plan's timetable, implementation processes and associated monitoring and reporting arrangements. Preparation, formalisation and monitoring of this action plan constitute a prerequisite for the effectiveness of the risk map.

410. Public sector entities with little or no experience of risk mapping exercises could, in their work towards a corruption risk map such as it is proposed in the previous paragraphs, usefully start with a priority examination of three processes that experience has shown to be particularly exposed to corruption risks: public procurement, human resources management and disbursement of subsidies (see Appendix 2).

Step 6: Formalising, updating and archiving the corruption risk map

411. All the above-mentioned elements combine to form the risk map. Its presentation is integral to staff's ownership of the map as a corruption risk steering tool.

412. The need to update the map should be assessed once a year.

413. Updates need to use the same method used to build the map, providing such method's risk identification, assessment, ranking and risk management procedures and methodologies offer the reasonable assurance that it truly reflects the public sector entity's real risk exposure.

414. It is recommended to keep all elements that can be used to assess the effective implementation of the mapping procedures and methodologies.

415. The different versions of the maps are dated, referenced and archived.

III.3) Third pillar: corruption risk management

A- Risk prevention

1. Rules on professional conduct/ethics and code of conduct

- **Definition and objectives of the code of conduct**

416. The code of conduct, whatever its given name, is a document that is an expression of senior management's decision to commit to a corruption prevention and detection approach. It may be incorporated into a system of "ethics" (such as a charter of ethics) or good conduct that may encompass more than the strict prevention of corruption, providing it is presented and disseminated in a manner that is perfectly understandable.

417. The code of conduct defines and illustrates with examples of the public sector entity's activities the different types of behaviour that are unacceptable since they are likely to constitute corruption.

- **Scope**

418. The code of conduct applies to all the entity's staff and managers as well as, where applicable in a suitable form, to the other elected officials and their staff.

419. The code should also be applicable to the public sector entity's other human resources (volunteers and trainees), in accordance with the relevant legal provisions.

- **Construction and approval process**

420. To demonstrate its commitment, senior management promotes the code of conduct and scrupulously applies its principles. Senior management's model conduct is key to the staff's sound application of the code of conduct.

421. The code of conduct, with a preface written by senior management, articulates senior management's values and commitment with respect to corruption prevention and detection. This leadership fosters the development of a culture of professional conduct, ethics, integrity and honesty.

422. The code of conduct for public sector entities whose staff are subject to the General Civil Service Regulations is signed by the department head after consulting with the technical committee or, in the future, the relevant social committee.

423. Where the public sector entity has rules of procedure, the code of conduct is incorporated into them and forms the subject, where appropriate, of a consultation procedure with the relevant bodies, authorities and departments.

- **Content**

424. The code of conduct should be written or updated following the corruption risk mapping, since the code of conduct describes the behaviour that is unacceptable based on the public sector entity's specific risks.

The code of conduct is not restricted to a set of good practices, but contains provisions on the types of unacceptable conduct that staff and managers are likely to encounter as a result of the public sector entity's activity. Entities are encouraged to structure the code of conduct into sections regarding the different types of unacceptable conduct.

425. The code of conduct also sets out and details how to comply with the ethical requirements applicable to the public sector entity's staff and managers.

426. Some of these requirements may be legislative or regulatory. The code of conduct may provide details on operational compliance with them. These requirements may also be usefully supplemented by the public sector entity's own measures in accordance with its risk profile.[11]

427. The code of conduct covers mainly gifts and invitations, conflicts of interest, rules on the use of the department's property and resources, and entertainment expenses. It can also detail:

- Moral and ethical obligations for public managers as referred to in Article 25 of Title 1 of the General Civil Service Regulations and Article 1 of the Transparency of Public Life Act 2013-907 of 11 October 2013;
- Provisions specific to certain categories of public servant (national security forces and the healthcare and welfare sector) where such are represented within the public sector entity;
- Provisions regarding disclosures of interests and assets applicable to the public sector entity;
- The applicable framework in terms of multiple jobholding and public servant mobility to the private sector and returns from the private sector to public service;
- All applicable rules to prevent conflicts of interest: recusal requirements and even voluntary declarations of non-conflict of interest or disclosure of interests;
- Prohibition of jobs for family members on elected officials' private office staff where relevant to the public sector entity;
- Rules governing holding multiple elected and administrative positions;
- The requirement for an accredited intermediary to manage the financial instruments for certain jobs and functions;
- Applicable transparency and freedom of information requirements with respect to the management of the public sector entity.

428. The code of conduct is illustrated by relevant examples of the public sector entity's activity and the risks defined in its corruption risk map (e.g. appropriate conduct with regard to hospitality from a supplier or by a person applying for a permit or authorisation).

429. If the public sector entity chooses a code of conduct that makes reference to "operational" factsheets or procedures which, without being part of the code itself, define, on the basis of the risk map, the operational details of conduct to be respected in order to manage risk situations, it is important that these documents form a consistent and clearly articulated whole guaranteed to be understood by and accessible to all staff members.

430. The code of conduct provides the name and contact details of the compliance officer (where applicable) and the whistleblower contact, who may be one and the same. In order to prevent any confusion between these two functions, the code of conduct specifies their respective roles and referral procedures.

[11] In the case of departments whose staff are subject to the General Civil Service Regulations, the department head exercises the power conferred by Article 25 of the Civil Servants' Rights and Obligations Act 83-634 of 13 July 1983: "All department heads may specify, following an opinion from staff representatives, the ethical principles applicable to staff under their authority, adapted to the department's assignments."

431. It presents the internal whistleblowing system designed to report conduct and situations in violation of the code of conduct liable to constitute corruption for staff subject to the General Civil Service Regulations.

432. The code of conduct states that breaches of its provisions are liable to incur disciplinary sanctions in accordance with its applicable provisions.

433. Staff subject to the General Civil Service Regulations who are found in breach of the measures set out in the code of conduct to organise the department and its activity are liable to incur a disciplinary sanction. Breaches of the legal ethical obligations mentioned in the code of conduct are also liable to incur a disciplinary sanction. Failure to comply with the code of conduct's recommendations corresponding to civil service regulations is also liable to incur a disciplinary sanction where it constitutes a breach of public servants' duty of honesty and integrity. Failure to comply with the recommendations of the code of conduct is a sign of corruption.

- **Code of conduct formalisation and accessibility**

434. The code of conduct written plainly in layman's terms is clear, to the point and unambiguous.

435. The code of conduct is disseminated in-house and forms an element of the public sector entity's staff and management training.

436. The code of conduct also serves as an external communication tool in relationships with users, suppliers and, more generally, the public sector entity's partners.

- **Updates**

437. The code of conduct is regularly updated, particularly following updates of the corruption risk map. To this end, the code of conduct needs to be dated.

2. Training and awareness

- **Definition and objectives**

438. As a vehicle for the public sector entity's culture of integrity, an effective and suitable training and awareness programme supports the broad dissemination of senior management's anti-corruption commitments, the staff's ownership of them and the building of a knowledge base shared by the different staff members.

439. An awareness programme results in more informed participants who are more receptive to the subjects presented to them.

440. A training programme consists of attaining the knowledge and skills required to undertake an activity or occupation. It is part of the public sector entity's general training plan.

441. The training and awareness programme needs to:

- Be coordinated with the other anti-corruption programme measures and procedures, such as the training course on the content of the code of conduct, the priority risk mapping foundation course for individuals identified as being at risk, the training and awareness course on the use of whistleblowing systems, etc.
- Address the particular risks to which the different staff categories are exposed.

- **An awareness programme for all staff**

442. Although the risk training programme prioritises managers and staff most at risk, an awareness programme is recommended for all personnel.

443. Awareness actions designed for all staff focus on:

- The code of conduct;
- Corruption in general, its implications, forms and associated disciplinary and criminal sanctions;
- Conduct to be adopted when encountering corruption and the role and responsibility of each individual;
- The internal whistleblowing system.

444. Whichever way these awareness actions are organised, their purpose is to advance awareness of the implications of corruption for the public sector entity and its environment.

- **Compulsory training for individuals most at risk**

445. Training for senior management, elected officials and their staff, and managers and staff most at risk informs them of both the due diligence required of them in the course of their activities and the conduct to be adopted when encountering high-risk situations.

446. The purpose of this training is for the individuals concerned to take ownership of the public sector entity's anti-corruption programme.

447. The ultimate effect is mitigation of the risks identified by the corruption risk map.

448. The human resources manager uses the corruption risk map, with the help of the manager or department in charge of the anti-corruption programme (or any other designated individual or department) where required, to identify the individuals most exposed to corruption risks, i.e. the individuals in charge of or involved in high-risk processes.

449. These may be, in particular:

- Senior management and elected officials (especially those with delegated authority);
- Managers and staff who have dealings with exposed third parties (purchasers, appraisers of applications for subsidies or authorisations, etc.);
- Staff taking part in the implementation of the anti-corruption programme.

450. Other elements, such as job descriptions, can be used as a basis for the identification of exposed managers and staff.

451. Training content varies depending on whether it is for managers and staff most exposed to the risks of corruption or other staff categories.

452. This content is adapted to the nature of the risks, the functions performed and the geographic areas in which the public sector entity works. It is regularly updated in association with the risk map updates.

453. The purpose of training is to improve understanding and knowledge of:

- Processes and their associated risks;
- Corruption offences;
- Due diligence required and measures to be taken to reduce these risks;
- Conduct to be adopted when encountering illicit solicitation;
- Disciplinary sanctions incurred in the event of non-compliant practices.

454. The common core of these training courses covers:

- The code of conduct;
- Corruption in general, its implications and forms;
- Applicable legal requirements and their associated sanctions;
- The anti-corruption programme;
- Conduct to be adopted when encountering corruption and the role and responsibility of each individual;
- The internal whistleblowing system.

455. Specific subjects are also addressed depending on the participants' functions and the specific risks they face. Corruption detection tools may be one subject covered by the training course for staff with control responsibilities.

456. The most exposed individuals are trained when they take up their positions. Regular training is provided throughout the exercise of their duties.

457. Training courses are given using suitable tools. Training courses must be accessible and suited to their target audience.

458. Training courses are practical and educational. Like the code of conduct, they use practical case studies and scenarios tailored to each audience and suited to the risks identified by the corruption risk map.

459. Members of the public sector entity may be asked to share their experiences in this area, their responses and their conclusions, thereby giving rise to discussion of operational constraints. Simulation exercises could be useful to help them take ownership of the rules in their day-to-day work.

460. The use of tools such as tests to check that participants have properly understood the training courses is to be encouraged. Such tests could be set during the training course or following a certain lapse of time to ensure that the knowledge has been assimilated.

461. Training courses may be taught by in-house staff or by an external service provider.

462. In the case of outsourcing, the public sector entity needs to take part in the design and running of the training course to ensure that its particularities are taken into account and that the training course's content is consistent with the policy deployed in the matter (e.g. elements regarding the code of conduct, risk map, etc.).

463. Lastly, corruption could also be addressed by more general training courses (public procurement, management, taking up a position of responsibility, training for elected officials, etc.).

- **Monitoring and control of the training programme**

464. Indicators are set up to monitor the training programme, including in the case of outsourced training. These indicators could include the following items:

- Percentage of target audience trained;
- Number of hours of training on the corruption prevention and detection programme.

465. Training programme quality and monitoring are checked, as is participant identification.

466. In the case of outsourcing of all or part of the training programme, the staff member or department responsible for the anti-corruption programme (or any other designated individual or department) must not only be informed of the training course timetable and educational content, but must also verify the effective deployment of the programme and the associated indicators.

3. Third-party due diligence

- **Definition and objectives of third-party due diligence**

467. Due diligence is conducted on the basis of the corruption risk map. Due diligence may concern, among others, the following third party categories: suppliers and sub-contractors, entities subsidised by the public sector entity, recipients of individual support, recipients of authorisations, partners or philanthropists, public service users, and any private or public sector entity r with which a given public sector entity has dealings in the course of its work, including entities with which it has regular dealings without having any de facto or de jure control over them (such as semi-public companies in which it has a minority shareholding).

468. The purpose of due diligence is to decide whether to enter into a relationship with a third party, continue with a relationship – with enhanced due diligence measures where necessary – or terminate a relationship.[12]

- **Definition of the third-party due diligence mechanism**

469. An exhaustive inventory of third parties, using an existing database where applicable, tends to facilitate the performance and management of third-party due diligence.

470. The database needs to be up to date and secure, which implies adopting formalised, secure procedures to create, approve, amend and delete third parties recorded in the database in strict accordance with the assigned tasks and authorisations.

471. The public sector entity needs to undertake an exhaustive inventory of its categories of third parties. The purpose of this approach is to determine *ex ante* the groups of third parties that expose it to corruption risks on the basis of the risk map.

472. The nature and depth of the due diligence to be conducted and the information to be collected are determined with respect to the different uniform groups of third parties with comparable risk profiles, as identified by the risk map. Consequently, the groups of third parties deemed to be risk-free or low-risk may require no due diligence or simplified due diligence, whereas groups deemed to present greater risks will require more thorough due diligence. Analysis of groups of third parties to determine those that can be ruled out for due diligence is particularly advisable for public services accessible to large numbers of users.

473. In each group of third parties requiring due diligence, due diligence is conducted on each third party separately according to its particularities, since the purpose of due diligence is to appraise the specific risk associated with the relationship or prospective relationship with a given third party.

474. Third-party due diligence enables the public sector entity to appraise individual situations, which the risk map (or even the third party's risk map) cannot do. A third party classed as a low-risk category on the risk map may be reclassified as a high-risk third party following its individual due diligence. Likewise, an incident, whistleblowing report or conviction concerning a third party in a category classified as low risk or whose behaviour changes in the course of a relationship may lead the public sector entity to perform more in-depth due diligence or to conduct due diligence as a matter of priority.

[12] Subject to compliance with the provisions governing the process under consideration.

- **Third-party due diligence in practice**

475. Three levels of players take part in due diligence:

- Staff in charge of and responsible for due diligence collect the information and documents useful for due diligence on the third parties with which they have a relationship or a prospective relationship. They issue a preliminary appraisal. This appraisal counts as a decision in cases judged to be low risk;
- The staff member or department in charge of the anti-corruption programme (or any other designated individual or department) provides expertise and advice to the staff in charge of due diligence and assists the operational level with its appraisals of and decisions on high-risk cases;
- Senior management decides on further action to be taken with respect to the highest-risk cases referred to it by the departments concerned.

476. The third-party due diligence procedure is formalised.

477. The public sector entity ascertains the information and documents useful for due diligence on the basis of its risk map. In many cases, part of the data listed below as a guideline is already requested by current administrative appraisal procedures.

478. As a guideline, due diligence can include:

- Collection of information by consulting the public sector entity's internal lists;
- Collection of open-source information, public documents and documents available to the public (e.g. press articles, financial statements, court rulings where published, control and inspection reports, etc.);
- A check to see whether the third party and its beneficial owners, such as they are defined by articles R. 561-1 and R. 561-2 of the Monetary and Financial Code, and its management or administrators appear on lists of sanctioned natural and legal persons (in particular, lists of persons debarred from public contracts funded by the World Bank and development banks, and the economic and finance ministries' list of persons subject to financial and international sanctions);
- Collection of information and documents from the third party by such means as a questionnaire, interview, audit and in-house approval or certification process.

479. The information is obtained in accordance with the applicable regulations, especially those governing personal data protection.

480. The public sector entity notes the main elements that identify the third party: name, corporate name, the structure's legal form, date of establishment, number of employees, turnover, capital, activity sector(s), specialisation(s) (for service providers in particular) and geographic location.

481. The public sector entity ensures that the third party has the experience, credentials and expertise required to conduct its task. In this regard, it may ask the third party to provide it with the professional references it deems necessary based on the data already collected (date of establishment, date of launch of the activity, etc.). A lack of credentials or experience may be defined as an aggravating factor by the appraisal of the third party's risk level. In the case of third parties with contracting authority status, these checks are conducted in accordance with the public procurement code.

482. Personal data regarding the third party's integrity, potentially including corruption proceedings and/or convictions, must be collected with due regard to data protection standards.

483. The public sector entity could also check that the third party has deployed an anti-corruption programme. Where a third party says nothing about the implementation of such a programme when bound to do so by law and does not document it, this may be considered as a risk factor.

- **Assessment of the third party's risk level**

484. The public sector entity assesses the third party's risk level based on the collected information and documents and an analysis of the circumstances of the prospective relationship (or an analysis of the nature and purpose of the relationship).

485. Certain relationships involve an acute risk of corruption, such as in the case of a third party tasked with helping the public sector entity to procure contracts. This could encourage the third party to indulge in non-compliant practices that circumvent its anti-corruption programme.

486. The establishment of a long-term, high-value financial relationship may be considered a risk factor by the assessment of the third party's risk level. Likewise, the public sector entity's level of economic dependence on the third party or the third party's level of economic dependence on the public sector entity could constitute a risk.

487. The public sector entity checks that the cost of the deliverable is consistent with the nature and volume of the goods or services sold by the third party and in line with market prices. An inconsistency could be a warning signal and the reasons for it would need to be justified.

488. The payment of commissions for winning contracts represents a risk factor in the assessment of the third party's risk level.

489. The risk assessment considers the third party's conduct: for example, where a third party refuses to provide or delays providing requested information and/or documents, the assessment could consider this to be a risk factor.

- **Conclusions to be drawn from third-party due diligence**

490. Following the assessment of the risk level, it may be decided to:

- Approve the relationship – with or without enhanced due diligence measures;
- Terminate or refrain from proceeding with the relationship;[13]
- Postpone the decision (pending further assessments, for example).

491. The persons who make the decision within the public sector entity are clearly identified.

492. The absence of risk factors following an assessment does not guarantee that the relationship with the third party is absolutely devoid of risk. Conversely, the identification of risk factors does not rule out the relationship, but must lead the public sector entity to take suitable due diligence measures during the relationship.

- **Due diligence and prevention measures to be deployed during a relationship with a third party**

493. Given that corruption prevention and detection measures need to be adapted to each public sector entity's environment, it is up to the concerned entity to define the measures it considers to be consistent with its particularities.

[13] See footnote 12.

494. In this regard, the public sector entity may usefully envisage one or more of the following options:

- Inform the third party of the existence of its anti-corruption programme by communicating the code of conduct, for example;
- Train or raise the awareness of the third party about the risk;
- Strengthen collective decision-making;
- Strengthen internal control (especially approval from superiors);
- Require a written anti-corruption commitment from the third party or insert a clause enabling the public sector entity to terminate the contractual relationship in the event of corruption if the legal nature of the relationship with the third party so permits.

- **Monitoring the contractual relationship with the third party** The contractual relationship needs to be clearly established in order to monitor its sound execution.

496. In this respect, the public sector entity needs to have full visibility of the payments received from and made to third parties in order to ensure that price rates and terms of payment are in accordance with the contractual provisions.

- **Third-party due diligence and public procurement**

497. Third-party due diligence by public sector entities applying the Public Procurement Code must be conducted in accordance with the fundamental principles of public procurement: freedom of access to government contracts, equal treatment of bidders and transparency of procedures.

498. This due diligence includes the checks provided for by the Public Procurement Code: the public sector entity checks, in particular, for the existence of any measures that may exclude a bidder from the public procurement procedures:

- Exclusion of businesses that have been convicted of a certain number of offences, including bribery;
- Exclusions at the discretion of the buyer:
    - In the event of a bid creating a situation of a conflict of interest, where such conflict cannot be resolved by other means;
    - In the event of an attempt to influence the decision;
    - In the event of an attempt to obtain confidential information.

499. Due diligence on economic operators serves to adapt the relationship between the contracting authority and the third party or parties in the light of the identified risk. In the case of a high-risk third party or a sector identified as sensitive by the risk map, the public sector entity may take such prevention measures as to:

- Strengthen collective decision-making;
- Train staff in charge of preparing or supervising the contract;
- Arrange recusal, where necessary, of potential procurement players with a conflict of interest;
- Strengthen internal control (especially approvals from superiors);
- Maintain enhanced due diligence throughout the performance of a contract concluded with a third party assessed as high-risk.

500. Given that bid analysis criteria need to have a connection with the object of the contract or its performance terms, the introduction of criteria with respect to a bidding firm's anti-corruption commitment would only appear to be possible in residual cases. The addition of such criteria could expose the contracting authority to accusations of favouritism.

- **Renewing and updating third-party due diligence**

501. The due diligence process is repeated at regular intervals in accordance with the third party's category and level of risk. In this respect, it is useful to set a review date when entering into a relationship.

502. Where information on a third party's situation does not affect the public sector entity's risk level, the information on the third party is merely updated. However, if this information reveals a significant change in the third party's situation, such as a change of beneficial owners, a merger of two entities or the acquisition of a new entity, then new third-party due diligence is undertaken.

503. The review process is the occasion to ensure that the third party has respected its anti-corruption commitments throughout the relationship.

- **Filing information on third parties**

504. The entire third-party due diligence file and the record of changes must be kept on file for five years from the date of the end of the relationship (or from the date of an occasional transaction), save in the case of stricter legislation.

B- Detection

1. Internal whistleblowing system

- **Definition and objectives**

505. The internal whistleblowing system is the procedure that public sector entities implement to enable their staff to inform a dedicated contact person about conduct or situations that could be code of conduct violations so that they can be eliminated and the appropriate sanctions applied, where necessary (see Appendix 1).

506. The public sector entities required to implement appropriate procedures for receiving whistleblower reports made by staff or by external and occasional collaborators under the terms of Article 8 of the Act are: central government (central administrations, departments with responsibilities at the national level, devolved departments), municipalities with populations greater than 10,000, *départements* and regions, local governments mentioned in Article 72-3 of the Constitution, and public inter-municipal cooperation institutions with tax-levying powers that include one or more municipalities with populations greater than 10,000, independent public authorities with fifty or more employees and independent administrative authorities, along with any other public sector or private sector entity with fifty or more employees (public institutions, public interest groups, etc.).

507. These procedures must make it possible to report offences (Article 6 of the Act) and, consequently, concern situations constituting corruption.

508. Staff working for local governments, public institutions or entities that are not required to implement a procedure for receiving whistleblower reports may also report an offence in accordance with the procedure stipulated in Article 8 of the Act. This means they may report to their direct or indirect superiors.

509. The General Civil Service Regulations and the labour code provide protection for whistleblowers, provided they comply with the provisions of the Act when making reports (issues that may be covered by whistleblower reports and procedures).

510. Staff covered by the General Civil Service Regulations may also make a report about a conflict of interest to their superior or their compliance officer and be afforded the same protection. Reports may also be made in cases that may not constitute illegal taking of interest, but seem to be violations of civil service ethical requirements regarding conflicts of interest nonetheless.

511. AFA recommends implementing a single whistleblowing system that is not limited to fighting corruption in view of the provisions already in force and pending transposition of Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law.

512. However, if a whistleblower report reveals potential corruption, an internal investigation must be carried out.

- **Coordination of different whistleblowing systems** For the sake of simplicity, a single technical platform should be implemented when legally possible to receive whistleblower reports and dispatch them for appropriate processing when several different whistleblowing systems are in use.

514. Setting up a single technical platform for receiving reports means that, in addition to staff, external collaborators and casual workers[14], or professional associations, can make reports. The platform may also be made public.

- **Organisation of the whistleblowing system**

515. The internal whistleblowing system must be appropriate for the public sector entity's risk profile.

516. Management of the system (including the contact person) must be performed in-house or outsourced.

517. The internal whistleblowing system specifies the role of the superior, who must be able to guide and advise staff, except where the superior is the perpetrator of the reported conduct.

518. The public sector entity ensures that the persons responsible for processing whistleblower reports are trained to respect the confidentiality of the reports they process and that they do not have any conflicts of interest. It also ensures that supervisory personnel are trained.

519. The internal whistleblowing system is presented immediately to the public sector entity's new hires.

520. Management of the system, including the contact person function defined below, may be contracted out to a third party, provided the latter has the necessary competence for proper processing of whistleblower reports and the means to ensure confidentiality. The services provided for this purpose must be monitored regularly. The public sector entity ensures that the third party chosen is provided with the resources to process whistleblower reports and, more particularly, makes sure that the third party's access to the relevant departments of the public sector entity is facilitated.

521. The internal whistleblowing system is to be deployed so that it covers the entire scope of the public sector entity. The system is adapted to the specific features of the constituent entities (activity, size, local legislation, etc.).

- **Processing whistleblower reports**

522. The internal whistleblowing procedure must specify the different steps to be followed when making a report, the procedures for the recipient's processing of the report, the rights of the persons concerned (and more particularly the protection of their rights), and the security and protection measures for personal data.

523. The internal whistleblowing system identifies:

- The contact person designated to receive reports within the public sector entity and, the person responsible for processing reports, if it is not the same person;
- The measures taken to ensure whistleblowers' anonymity, the confidentiality of the reports and the persons named in them, even when investigation and processing of reports require communication with third parties. Breach of confidentiality must be liable to disciplinary sanctions.

524. The whistleblowing system is secure and access privileges are restricted to personnel authorised to receive and process the reports.

[14] External collaborators and casual workers include temporary staff, interns, service providers, subcontractors' employees, etc.).

525. If one or more persons are implicated, the public sector entity must take care about gathering evidence and documents, particularly when the persons named in the report are able to destroy incriminating data or documents.

526. The internal whistleblowing system specifies the procedures for access to the system and exchanging information with the whistleblower, more specifically:

- The channels for making reports: they could be a dedicated e-mail address, management software, or even a specific ethics platform. The report can also be submitted through the whistleblower's superiors. In all events, these channels must be easily accessible;
- Procedures for whistleblowers to provide information and documents to back up their reports;
- In the event of an internal investigation, the business information and documents submitted by the whistleblower that may be used for this purpose;
- The provisions made to notify the whistleblower immediately of reception of the report and of the time needed to determine its admissibility. For this purpose, it should be stated that the acknowledgement of receipt does not mean the report is admissible.
- The provisions made to notify the whistleblower, and, where necessary, the persons named in the report, that the procedure is closed.

527. If automated report processing is introduced, the procedure must indicate the provisions that ensure compliance with the terms of the Data Protection Act 78-17 of 6 January 1978 and other personal data protection provisions. Personal data means any information about a natural person who is identified or identifiable.

528. In the face of growing numbers of requirements with regard to receiving reports, the French Data Protection Authority (CNIL) published its ruling 2019-139 dated 18 July 2019 setting standards for handling personal data for the purpose of implementing a whistleblowing system.

529. Reports may be submitted anonymously. The system must make it possible to continue dialoguing with the whistleblower while still maintaining their anonymity (for example, whistleblowers could be asked to provide an anonymous email address or a post office box address).

530. It is essential to define and formalise the internal investigation procedure before the system is launched, while being vigilant about the choice of investigation participants and the conduct of investigations. The investigation procedure may specify:

- The criteria for initiating an investigation;
- The procedures for conducting an investigation.

531. The persons responsible for conducting the investigation must be bound by very strict confidentiality obligations, which need to be formalised.

532. If the investigation is outsourced, the services rendered by the selected provider must be monitored regularly for compliance with the confidentiality and data protection rules.

533. Any internal investigation is conducted by one or more qualified persons to be designated by the public sector entity's senior management.

534. Senior management is systematically informed about investigations opened into the most sensitive situations, with the exception of situations where senior management itself is implicated.

535. After the internal investigation, an official investigation report is drafted to present all of the facts and evidence gathered to substantiate or allay suspicions, and to describe the method used. The internal investigation report draws conclusions about any further action needed on the whistleblower's report.

536. If the suspicions seem to be substantiated, the report is submitted to senior management (or the supervisory body if senior management is implicated) for further action.

537. If the internal investigation proves conduct contrary to the code of conduct, the disciplinary sanctions provided for such cases must be imposed, as decided by senior management.

538. Legal proceedings may also be instigated against the natural person implicated, if the public sector entity decides to notify the judicial authorities by means of a complaint or a report. This notification is mandatory if the public sector entity is subject to the authorities listed in Article 40 of the Code of Criminal Procedure.

539. The reports must be used to update the risk map, while maintaining the confidentiality ensured by the system, and to draw conclusions with regard to improvements to be made to elements of the anti-corruption programme (training programme, code of conduct, third-party due diligence).

- **Implementation of the internal whistleblowing system**

540. The following steps can be helpful:

- Establishing a formalised procedure that may include the appointment of a whistleblower contact and the creation of a committee of qualified persons bound by confidentiality obligations. The committee decides collectively on any further action to be taken on whistleblower reports;
- Including a chapter on the whistleblowing system in the code of conduct with reference to the said procedure;
- Disseminating the internal whistleblowing procedure to all staff by all means (letter from senior management, posters, intranet site, handouts, etc.) to ensure that everyone concerned knows about the system and has access to it. If the anti-corruption whistleblowing system is part of a system meeting other legal requirements, the procedure must also be disseminated to the occasional collaborators of the public sector entity. The public sector entity may decide to make its whistleblowing system accessible to third parties. The public sector entity may choose to use its external communication tools, such as websites and documents provided to third parties, to talk about its whistleblowing system;
- Presenting the whistleblowing system to all staff as part of awareness-raising actions;
- Training the staff tasked with receiving, managing and processing whistleblower reports, with particular emphasis on confidentiality obligations and training the staff with the greatest risk exposure;
- Establishing first- and second-line-of-defence monitoring of the internal whistleblowing system and incorporation of this system into the internal audit plan as part of the third line of defence. The three lines of defence mentioned above may be adapted to avoid any conflicts of interest or self-auditing. When necessary, it is important for the staff processing a whistleblower report to be different from the staff who monitor processing and for an ex-post audit to be conducted;
- Implementing indicators to assess the quality and effectiveness of the whistleblowing system (including the number of reports received, shelved or processed, processing times, problems raised). These indicators are submitted to senior management.

- **Archiving whistleblower reports and their follow-up**

541. The retention and archiving periods for personal data relating to whistleblower reports differ depending on whether further action is taken.

542. If the processing manager decides to take further action[15] on a whistleblower report, or if disciplinary action or litigation is initiated, all of the personal data collected during the investigation may be retained until the end of the proceedings, up to the statute of limitations (six years), or until all appeals have been exhausted.

543. If the investigation of a whistleblower report does not lead to any further action, personal data must be destroyed within two months of closing the investigation.

544. When whistleblower reports are received through a single technical platform and they do not relate to conduct that could be qualified as corruption, the retention periods are determined by Decree 2017-564 of 19 April 2017 on the procedures for receiving whistleblower reports within public sector entities, private sector entities and central government administrations.

545. The internal whistleblowing procedure (Articles 8 or 17 of the Act) is distinct from the report to the public prosecutor mentioned in Article 40 of the Code of Criminal Procedure[16].

546. Several criteria must be met to make a report to the public prosecutor under the terms of Article 40:

- The reported conduct must constitute a crime or misdemeanour;
- It must be "adequately substantiated";
- The staff member must have gained knowledge of them in the performance of their duties.

2. Internal control of corruption risks

- **Contribution of the internal control and audit system to the prevention and detection of corruption**

547. Public sector entities may already have internal control and audit systems that are not specifically designed for corruption risks. These systems may have up to three lines of defence:

- The purpose of the first line of defence[17] is to ensure that the tasks that are part of an operational or support process are performed in compliance with the public sector entity's procedures. These controls may be performed by the operational or support staff or by their superiors;
- The purpose of the second line of defence[18] is to ensure that the first-line-of-defence controls are properly executed. These controls may be conducted at prescribed intervals or randomly. The controls for this line of defence are conducted by a different department than the ones that implement the operational and support processes from day to day. These controls may be performed by the risk management, quality control, management control or compliance departments, etc.

  The controls for the first and second lines of defence of the internal control system are formalised under a procedure that specifies the identified high-risk processes and situations, the frequency of controls and control procedures, the persons responsible for controls and the procedures for submitting their findings to senior management.

[15] See footnote 4.

[16] Article 40 of the Code of Criminal Procedure: "*Every constituted authority, every public officer or civil servant who, in the performance of their duties, gains knowledge of a felony or of a misdemeanour is obliged to notify the public prosecutor forthwith and provide the prosecutor with any relevant information, official reports or documents*."

[17] See footnote 5.

[18] See footnote 6.

- The purpose of the third line of defence, also known as "internal audit", is to ensure that the control system complies with the public sector entity's requirements and is implemented effectively and kept up to date.

548. The programme for managing corruption risks is part of the public sector entity's internal control system. It builds on pre-existing risk management systems (for financial risks and operating risks, in particular), which can be put to use immediately for preventing, detecting and managing certain corruption risks. AFA recommends that public sector entities supplement their internal control procedures on the basis of the corruption risk map to ensure appropriate attention is given to such risks.

549. The corruption risk map, along with the associated action plan, internal control plan and internal audit plan, enhance the overall internal control and audit system that does not specifically address the public sector entity's corruption risks.

550. The internal accounting control system, which often predates the specific corruption risk management programme, plays a special role in preventing and detecting corruption. With this in mind, care should be taken to ensure it is properly deployed.

- **Accounting controls**

551. The reliability of public accounts is a foundational principle of public finance[19]. Similarly, the principle of segregation of authorising officers and accountants is specific to public sector entities. Under this principle, the authorising officer approves financial transactions and the accountant executes them and records them in the accounts, after verifying their lawfulness. Only the accountant handles the funds. The accountant also monitors publicly-managed enterprises. The purpose of segregating authorising officers' and public accountants' duties is to ensure sound and honest management of public funds. The purpose of the public accountants' verifications is to catch any errors or irregularities before payments are disbursed. Public accounts have a critical role to play in detecting corruption. Corruption risk must be considered when determining the methodology for supervisory control of expenditure and streamlined control in partnerships.

552. Authorising officers' accounting control and audit procedures constitute an important instrument for preventing and detecting corruption. They contribute to risk management as part of the internal control and audit procedures. A key factor for their effectiveness is the use of reliable and user-friendly financial information systems.

553. Internal accounting control provides reasonable assurance about the quality of accounts, meaning they provide a true and fair view of the economic situation, assets and finances. The internal control system includes an internal accounting and financial audit conducted by a separate department to evaluate the effectiveness of the internal control system periodically.

554. Even if an independent third party (such as a financial jurisdiction) audits their financial statements, the public sector entities concerned are still required to implement and perform internal controls to ensure the reliability of their financial information and to manage their risks.

[19] Article 47-2 of the Constitution enshrines the principles of accuracy, lawfulness and reliability of accounts for all public administrations.

- Definition and objectives

555. The purpose of the accounting controls, hereinafter "anti-corruption accounting controls" is to ensure that the accounts are not used to conceal corruption.

- Coordination with existing accounting controls

556. Public sector entities have general-purpose accounting control procedures to provide reasonable assurance about the quality of accounting information. These procedures ensure the lawfulness, accuracy and reliability of the accounts and financial statements.

557. Anti-corruption accounting controls:

- Ultimately ensure compliance with the same principles as general-purpose accounting controls (lawfulness, accuracy and reliability of the accounts and financial statements);
- Use the same methods as general-purpose accounting controls, including sampling, consistency reviews, physical inventory counts and third-party confirmations.

558. The procedures are defined with regard to the high-risk situations highlighted by the public sector entity's corruption risk mapping exercise to enhance or supplement the existing general-purpose controls.

559. Examples of high-risk situations to be addressed by these procedures include entertainment and travel expenses, processing of requests for funds, management of real property and inventories, operations of government-funded enterprises, products and services and central government property, and off-balance sheet commitments.

- Formalising anti-corruption accounting controls

560. Anti-corruption accounting control procedures are formalised under a procedure that sets out:

- Their purpose and scope;
- Roles and responsibilities for their implementation;
- Sampling procedures for transactions subject to controls, as appropriate;
- Defining a control plan;
- Procedures for managing incidents;
- Thresholds and materiality criteria that trigger audits.

- Content of anti-corruption accounting controls

561. The anti-corruption controls for the first line of defence are generally performed by the persons responsible for entering and approving accounting entries. These persons ensure that the entries are properly justified and documented (especially manual entries).

562. High-risk accounting entries should be reviewed and approved by a staff member who is independent from the person making the entries in order to mitigate the risks associated with self-auditing.

563. Crosschecks between staff members are satisfactory for entries involving sums under a set threshold. Entries for greater amounts require approval by a superior.

564. The accounting anti-corruption controls for the second line of defence are performed all year long by persons who are independent from those who performed the controls for the first line of defence.

565. The purpose of these controls is to ensure proper performance of the anti-corruption accounting controls for the first line of defence. When sampling is used, the sampling method must be representative of the risks incurred in the transactions (including manual entries, approval authority and segregation of duties).

The sampling procedures are defined with regard to a prior analysis of the various entries and risks incurred to ensure representativeness.

566. If the anti-corruption accounting controls for the first line of defence are automated, the controls for the second line of defence should be adapted in consequence.

567. The findings of the anti-corruption accounting controls for the second line of defence are summarised with the definition of corrective actions as part of an action plan if any problems are found.

568. The effectiveness of anti-corruption accounting controls is assessed on a regular basis as part of the accounting controls for the third line of defence, which are also called "accounting audits".

569. Such accounting audits cover the whole accounting system to ensure that the anti-corruption accounting controls comply with the public sector entity's requirements, are effectively implemented and kept up to date.

570. For this purpose, the accounting audits assess the appropriateness and effectiveness:

- Of governance and resources for anti-corruption accounting controls;
- Of the methods (particularly the integration of the corruption risk map) and application of anti-corruption accounting controls for the first and second lines of defence.

▪ <u>Treating problems found</u>

571. If a problem is found, certain existing accounting procedures may be supplemented to correct the problem.

572. Problems found also contribute to updating the corruption risk map and may be presented as additional examples to illustrate the code of conduct and training materials on preventing corruption.

573. If the problem stems from a failure in the implementation of procedures or the anti-corruption programme, the superior may consider taking measures against the person responsible for the failure. These measures may range from a reminder about the rules to a sanction, depending on the severity of the failure.

574. If the problem leads to suspicions or reveals cases of corruption, it must be reported to senior management, which may decide to launch an administrative investigation.

C – Internal monitoring and evaluation of the anti-corruption programme

1. Purposes and procedures

575. The public sector entity monitors and evaluates the corruption prevention and detection procedures to ensure that they are adequate and effective.

576. This system meets four objectives:

- Monitor the implementation of corruption prevention and detection measures and test their effectiveness;
- Identify and understand any deficiencies in the implementation of the measures and procedures;
- Define, where necessary, recommendations or other suitable corrective measures to improve the programme's effectiveness;
- Detect any corruption.

577. Each monitoring activity needs to specify:

- Purpose and scope;
- The person(s) responsible;
- The method used (type of measurement and supporting, analytic and evaluation documents), the sampling procedures, where applicable, based on a risk analysis, frequency and formalisation specifications;
- Submission of the monitoring findings and potential corrective measures;
- The monitoring record retention procedures.

578. The adequacy and effectiveness of the anti-corruption programme's measures and procedures are regularly evaluated by third-line-of-defence audits. These internal audits ensure that the anti-corruption programme complies with the public sector entity's requirements, is implemented effectively and is kept up to date. The internal audit is also asked to ensure that the risk situations identified by the corruption risk map are covered by effective prevention measures.

2. Typology of monitoring

579. Each anti-corruption programme measure and procedure is subject to monitoring.

580. AFA recommends that this monitoring focus on the following elements:

Procedure	Focal points
Corruption risk mapping	- Regularly check the adequacy of the map's scope, the methodology used and the deployment of the associated action plans; - Analyse deficiencies found, especially incidents that have occurred, in order to update the map.
Code of conduct and associated policies/procedures	- Ensure that procedures (e.g. acceptance of gifts and invitations) are actually implemented with ex ante and ex post audits on samples; - Ensure that the code of conduct is disseminated and that the persons concerned know and understand it; - Regularly check the suitability of the code of conduct and the examples of situations and conduct described in the code (particularly if incidents have been reported and when updating the risk map).
Training	- Ensure that the planned training has actually been provided and taken by the persons concerned (especially particularly exposed individuals and individuals in charge of implementing the anti-corruption procedures); - Check the consistency of training content with regard to target audiences and their risk exposure as identified by the map.
Third-party due diligence	- Check the effective implementation of due diligence measures with ex ante and ex post audits on samples; - Regularly check that third-party due diligence matches the risks identified by the map.
Internal whistleblowing system	- Monitor the deployment and correct use of the whistleblowing procedure; - Conduct a qualitative and quantitative analysis of the whistleblowing reports received over the period (channels used, any reports received through other unidentified channels, subject matter, etc.); - Check the adequacy of the responses to the reports received; - Check the report archiving procedures.
Internal control and accounting controls	- Check the formalisation of the control procedures; - Monitor the effective implementation of the controls provided for and their traceability; - Regularly check that internal control is adequate for the risks identified on the map.

Disciplinary rules	- Check that appropriate disciplinary action is taken for any breach of the code of conduct or corruption.

581. First-line-of-defence monitoring is formalised and documented.

582. A formalised audit plan is drawn up for second-line-of-defence monitoring describing the scope, roles and responsibilities, frequency, sampling procedures, formalisation specifications, follow-up on irregularities and associated action plans.

583. A formalised audit programme is drawn up for third-line-of-defence audits describing the scope, sampling procedures, formalisation specifications, follow-up on irregularities and associated action plans.

3. Management of deficiencies found and follow-up on recommendations

584. These deficiencies may lead senior management to impose appropriate and proportionate disciplinary sanctions on their perpetrators.

D- Corrective action

1. Management of and follow-up on deficiencies found

585. Deficiencies associated with the implementation of procedures – and potentially flagged by the monitoring and audits – are analysed to identify their cause and correct them.

2. Disciplinary rules

- **Definition**

586. The disciplinary rules correspond to the sanctions that a public sector entity may take against a staff member for misconduct.

587. The main types of misconduct considered as grounds for a disciplinary sanction are corruption, violation of the code of conduct[20] and breach of the duty of integrity.

- **Principle of a scale of sanctions**

588. The disciplinary sanction must be proportionate to the misconduct as set out in the scale of sanctions provided for by the applicable disciplinary rules.

- **Mechanism**

589. Senior management's involvement in corruption risk management entails taking disciplinary action and imposing proportionate disciplinary sanctions in the event of corrupt conduct, violation of the code of conduct[21] or breach of the duty of integrity.

590. Depending on the case, charges may be pressed or the public prosecutor notified under the terms of Article 40 of the Code of Criminal Procedure at the time of the instigation of disciplinary action.

591. Senior management is not bound to wait for the criminal ruling before imposing disciplinary sanctions if the misconduct is proved and serious enough to warrant sanctions. Disciplinary sanctions may be imposed on the basis of the findings of a detailed internal investigation that firmly establish the materiality of the accused person's misconduct.

592. In the case of the code of conduct applicable to elected officials, it is for senior management to decide on the action to be taken for non-compliance by an elected official with the provisions of this code. This could, in certain cases, give rise to a change to, if not withdrawal of the elected official's delegated authority and exclusion from certain bodies such as the tender committee.

- **Creation of a sanctions list**

593. A list of disciplinary sanctions imposed on the entity's staff helps strengthen corruption risk management mechanisms.

594. Irrespective of the medium used to publish this list, the public sector entity ensures the strict confidentiality of its content and compiles it in accordance with the personal data protection rules.

[20] Subject to the specifications in paragraph 433 above for staff governed by the General Civil Service Regulations.
[21] See footnote 20.

- **internal communication**

595. Senior management may request the dissemination of disciplinary sanctions in a way that guarantees total anonymity so as to serve as a reminder of its policy of zero tolerance for any corruption or misconduct.

APPENDIX 1: Whistleblowers[22]

596. The system of protection for whistleblowers necessitates ensuring that their rights are protected, including the strict confidentiality of their identity, as well as the matters disclosed and the persons named in the whistleblowing report. Breach of confidentiality must be liable to disciplinary sanctions.

597. In addition to setting up a whistleblowing report reception system, anyone seeking to report a breach of Article 6 of the Act can report it to their direct or indirect superior or to a whistleblower contact appointed by the employer.

598. If the person who receives the whistleblowing report does not act on it within a reasonable space of time, the whistleblower may then refer the matter to the legal or administrative authorities or professional bodies.

599. The whistleblower may also refer the matter to the Defender of Rights ("*Défenseur des droits*")for the whistleblowing report to be directed to the appropriate body.

600. If none of the bodies to which the whistleblowing report is made has addressed it within three months, the report may be made public.

601. In the event of grave, imminent danger or risk of irreversible harm, the report of a breach of Article 6 of the Act may be referred directly to the legal or administrative authorities or professional bodies. It may also be made public.

[22] https://defenseurdesdroits.fr/

APPENDIX 2: Example of risk scenarios for public sector entities

AFA has identified examples of risk scenarios in the following three public management processes:

- Disbursement of subsidies;
- Human resources management;
- Public procurement.

At the same time, it has identified examples of prevention and detection measures along with best practices for risk mitigation. As stated in paragraph 410 of these guidelines, AFA suggests that public sector entities, especially those not familiar with risk mapping, prioritise the examination of these public management processes at the start of their mapping exercise.

These examples are not exhaustive and are to be adapted and rounded out in accordance with each public sector entity's risk profile.

NB: This appendix is an integral explanatory and illustrative part of the guidelines for public sector entities.

1- Disbursement of subsidies

1.1 Main corruption risks associated with granting subsidies

The allocation of subsidies is particularly exposed to the risks of **misappropriation of public funds** and **unlawful taking of interest**:

Misappropriation of public funds:

- ✓ In the case of a subsidy granted to a "shell" company.
- ✓ When the subsidy is disbursed despite an incomplete application.
- ✓ When the public funds are disbursed not to the applicant association, but to a third party that has substituted its own bank details for the association's.
- ✓ When the association allocates all or part of the public funds received to a use other than that for which the subsidy was granted.

Unlawful taking of interest:

- ✓ When the application is appraised by a public servant who has an interest in whether or not the subsidy is granted (for example, when his or her spouse is on the board of the association).
- ✓ When the person who decides to grant the subsidy or who participates in a collective decision to grant the subsidy has an interest in whether or not the subsidy is granted.

1.2 Examples of corruption prevention and detection measures in the subsidy disbursement process

- ✓ Train public servants and elected officials in the management of conflicts of interest and solution options: recusal, abstention from appraisal, etc.
- ✓ Design the subsidy application form to be able to verify the existence of the applicant body, the reality of its activity and the identity of its managers.
- ✓ Conduct a public awareness survey on the applicant.
- ✓ Introduce a systematic check to match the identity of the subsidy recipient and the identity of the holder of the bank account receiving the funds.
- ✓ Do not disburse the entire subsidy amount immediately and make the subsequent disbursement(s) subject to an interim management report; conduct on-site audits.
- ✓ Provide for a requirement to account for the use of the subsidy.
- ✓ Conduct audits, which may rely on sampling methods, of the appraisal of subsidy applications.

2- Human resources management

2.1 Main corruption risks associated with human resources management

Human resources management is particularly exposed to the risks of **bribery**, **influence peddling**, **unlawful taking of interest**, **misappropriation of public funds** and **extortion by public officials** in its recruitment, career management and payroll activities.

Bribery and influence peddling:

- ✓ When a hiring decision is made in return for a benefit granted to the recruiter or to a person who exercises an influence over the recruiter.

Unlawful taking of interest:

- ✓ When a recruiter or hiring committee member does not disclose personal ties to an applicant and participates in the decision-making process regarding that applicant's recruitment or promotion.

Misappropriation of public funds:

- ✓ When the person hired and paid does not work for the public sector entity (fake job).
- ✓ When a career or payroll manager creates a fake staff member in the human resources management information system and associates his or her own bank account with the fake staff member, thereby receiving compensation for a fake job.

Extortion by public officials:

- ✓ When a public servant declares overtime that has not been worked in order to be paid the relevant compensation.
- ✓ When a public servant receives undue grade-related compensation after having deliberately provided false information that reconstitutes his or her career history to his or her advantage.

2.2 Examples of corruption prevention and detection measures in the human resources management process

- ✓ Train staff in the management of conflicts of interest in recruitment and organise widespread access to the compliance officer for advice on the matter.
- ✓ Regularly crosscheck pay slips with the names on the department's organisation chart.
- ✓ Optimise automatic calculation of promotions and reclassification in the human resources management information system and provide for approval from a superior for manual overrides.
- ✓ Prevent access privileges for staff enabling them to make changes to their own files in the human resources management information system.
- ✓ Systematically check for unusual changes in pay for one and the same staff member.
- ✓ Organise audits on samples of data entries by peers and superiors.
- ✓ Organise a regular rotation of staff members in positions particularly exposed to corruption risks.

3- Public procurement

3.1 Main corruption risks associated with public procurement

The award of public contracts is particularly exposed to the risks of **bribery** and **influence peddling**:

- ✓ A contract is awarded in return for a sum the bidder pays to the decision-maker (bribery) or that the bidder is asked to pay to influence a government decision-maker (influence peddling).

Non-compliance with the principles of public procurement in itself constitutes corruption in the form of **favouritism**. These principles are free and equal access by bidders to government contracts and transparency of procedures. The risk of favouritism covers many types of situations:

- ✓ Inappropriate choice of bidding procedure.
- ✓ Unjustified use of special procedures (urgent need/contract negotiated without competitive bidding).
- ✓ More favourable treatment of one of the organisations during bidding procedures (communication of inside information, for example).
- ✓ Biased or "leading" choice of bid analysis criteria.
- ✓ Misuse of additions to contracts.

The decision to award a public contract can also lead to **unlawful taking of interest** when the decision-maker or one of the decision-makers has any kind of interest in a bidder or the company awarded the contract:

- ✓ An elected official sits on the tender committee when one of the bidders is owned by a family member, even if the bid in question is not chosen.

Lastly, there is a risk of **misappropriation of public funds** in the performance of a public contract:

- ✓ Payment for services or work ordered, but not delivered.
- ✓ An addition to the contract drawn up in breach of public procurement rules.
- ✓ Payment for all the services or work ordered when delivery was partial.

3.2 Examples of corruption prevention and detection measures in public procurement

- ✓ Choice of bidding procedure: compliance with the entity's rules for amended procedure contracts (thresholds) and strict application of the criteria justifying the use of special procedures.
- ✓ Bidding: provide the same level of information to all bidders and justify the choice of bid analysis criteria, including technical criteria.
- ✓ Contract award: introduce recusal for decision-makers with an interest (financial or moral) and use collective decision-making to award amended procedure contracts.
- ✓ Performance: pay particular attention to delivery and regularly verify the services and work actually delivered (volume and quality).