Guidelines to help private and public sector entities prevent and detect corruption, influence peddling, extortion by public officials, unlawful taking of interest, misappropriation of public funds and favouritism

Version 12-2017

French Anti-Corruption Agency guidelines to help private and public sector entities prevent and detect corruption, influence peddling, extortion by public officials, unlawful taking of interest, misappropriation of public funds and favouritism

Contents

Scope of the French Anticorruption Agency Guidelines

Under the terms of Article 3-2° of the Transparency, Anti-Corruption and Economic Modernisation Act 2016-1691 of 9 December 2016, the French Anti-Corruption Agency (AFA) "*shall draft guidelines to help private and public sector entities prevent and detect corruption, influence peddling, extortion by public officials, unlawful taking of interest, misappropriation of public funds and favouritism*[1]*."*

Hereinafter, these offences are referred to using the generic term "*corruption*".

The Agency's Guidelines are inspired by the best international standards. These Guidelines complete the arrangements established by the abovementioned Act of 9 December 2016 and are France's official anti-corruption policy framework. The Guidelines are applicable everywhere on French territory. They contribute to the implementation of France's international commitments in the fight against corruption.

These Guidelines are intended for all private and public sector entities, regardless of their size, legal structure, business area, revenue or number of employees. These entities are called "*organisations*" hereinafter. In view of the importance of the matters covered by the Agency's Guidelines, they are also applicable to unincorporated entities.

1. Entities Concerned by the Agency's Guidelines

Within the meaning of these Guidelines:

- Private sector entities mean:

  - public limited companies, simplified joint-stock corporations, limited liability companies, professional partnerships;

  - economic interest groupings (EIGs);

  - non-profit organisations governed by the Act of 1 July 1901 on the conditions for forming these organisations;

  - foundations.

The Guidelines apply to all companies, including subsidiaries of foreign groups, if such subsidiaries are established in the French Republic.

The Guidelines are also intended for all of the abovementioned corporations and entities, regardless of where they do business, including other countries that do not have more rigorous standards for preventing and detecting corruption.

- Public sector entities mean:

  - Central government (constitutional public authorities, central administrations, devolved central government administrations, departments with national scope, independent administrative authorities, etc.);

  - local governments and groups of local governments;

1. *See Appendix for definitions.*

- public establishments;

- public interest groups (GIPs).

2. Objectives

The Agency's Guidelines are aimed at helping:

- organisations adopt suitable operating rules to strengthen their performance or their competitiveness and to protect themselves against harm to their reputation or economic value arising from an impairment of their probity.
- public industrial and trading establishments subject to Article 17 of Act 2016-1691 of 9 December 2016[2] to comply with their obligations;
- organisations to prevent a penalty imposed by a foreign authority for failure to comply with an obligation to prevent or detect corruption.

After public consultation, the Agency's Guidelines will be updated periodically in accordance with Article 3-2° of Act 2016-1691 of 9 December 2016.

3. Legal Force of the Agency's Guidelines

Under the terms of the Act of 9 December 2016, the Agency's Guidelines shall be published in the Official Journal, but they are not legally binding.

The Agency's Guidelines provide the language for organisations to define their anti-corruption compliance programmes as part of their risk management strategy, including management of reputation risk and business risk.

4. Adapting the Guidelines to the Specific Needs of Each Organisation

These anti-corruption Guidelines are a coherent and indivisible policy framework applicable to all organisations, regardless of size, legal structure, business area, revenue or number of employees.

However, organisations must still adjust and adapt these standards according to their own risks, business models and issues. Accordingly, the more uniform the business activities and the more rational the business model, the more concentrated the issues at stake and risk exposures will be and the more affordable and proportionate the cost of risk management will be.

Corruption risk mapping identifies risks that will determine the contents and level of detail of organisations' anti-corruption compliance programmes. This means that organisations' compliance efforts should prioritise risk mapping.

2. *The obligation to implement the measures and procedures stipulated in Article 17 of Act 2016-1691 of 9 December 2016 applies to chairpersons, managing directors and managers of the companies covered by the Article. Following the French Anti-Corruption Agency Recommendations could help them fulfil this obligation.*

DEFINITIONS

Corruption is defined as an act whereby a person holding a specific public or private sector function, solicits or proffers or accepts or gives a gift, offer or promise to carry out, obstruct or abstain from carrying out an act pertaining directly or indirectly to his function. **The offence of corruption** is established by Articles 433-1 and 433-2 of the French Criminal Code.

Influence peddling is defined as "The direct or indirect request or acceptance without right and at any time of offers, promises, donations, gifts or advantages for oneself or others, when done by a person holding public authority or discharging a public service mission, or by a person holding a public electoral mandate: to carry out or abstain from carrying out an act relating to his office, duty, or mandate, or facilitated by his office, duty or mandate; or to abuse his real or alleged influence with a view to obtaining from any public body or administration any distinction, employment, contract or any other favourable decision." **The offence of influence peddling** is established by Article 432-11 of the French Criminal Code.

Extortion by public officials is defined as any acceptance, request or order to pay as public duties, contributions, taxes or impositions any sum known not to be due, or known to exceed what is due, committed by a person holding public authority or discharging a public service mission. **The offence of extortion by public officials** is established by Article 432-10 of the French Criminal Code.

Unlawful taking of interest is defined as the taking, receiving or keeping of any interest in a business or business operation, either directly or indirectly, by a person holding public authority or discharging a public service mission, or by a person holding a public electoral mandate who at the time in question has the duty of ensuring, in whole or in part, its supervision, management, liquidation or payment. **The offence of unlawful taking of interest** is established by Article 432-12 and Article 432-13 of the French Criminal Code.

Misappropriation of public funds is defined as the destruction, misappropriation or purloining of a document or security, of private or public funds, papers, documents or securities representing such funds, or of any object entrusted to him as part of his function or tasks, committed by a person holding public authority or discharging a public service mission, a public accountant, a public depositary or any of his subordinates. **The offence of misappropriation of public funds** is established by Article 432-15 of the French Criminal Code.

Favouritism is defined as an offence committed by a person holding public authority or discharging a public service mission or holding a public electoral mandate or acting as a representative, administrator or agent of central government, local government, public establishments, national semi-public companies discharging public service missions and local semi-public companies, or any person acting on behalf of any of the above-mentioned persons, who obtains or attempts to obtain for others an unjustified advantage by an act breaching the statutory or regulatory provisions designed to ensure freedom of access and equal treatment for bidders in tenders for public contracts and delegated public services. **The offence of favouritism** is established by Article 432-14 of the French Criminal Code.

Top management's Commitment to Preventing and Detecting corruption

Top management's commitment to a zero-tolerance policy for any behaviour that is unethical in general, and any risk of corruption more specifically, is fundamental to any strategy for preventing and detecting corruption.

Top management's commitment demonstrates the organisation's determination to ensure and promote business behaviour and ethics that meet strict integrity rules, even when preventing and detecting corruption requires the use of specific resources that could affect the organisation's operations.

1. Definition and Purpose of Top management's Commitment

Implementation of a risk management strategy and an anti-corruption compliance programme relies on top management's commitment to establish a culture of integrity, transparency and compliance.

This commitment takes the form of approval of a corruption prevention and detection system, as well as a corporate code of conduct. The anti-corruption code of conduct testifies to top management's decision at the highest level to commit the organisation to preventing and detecting corruption.

2. Contents of Top management's Commitment

The French Anti-Corruption Agency recommends that top management's commitment to a corruption prevention and detection policy be based on four pillars.

2.1. Adopting a zero-tolerance policy for corruption risk

Within the organisation and in its dealings with third parties, top management:

- should make preventing and detecting corruption a priority for the organisation;

- should make sure that the resources allocated to preventing and detecting corruption are proportionate to the risks;

- should adopt a firm attitude to any cases of corruption. The drafting of disciplinary rules and enforcement of sanctions are concrete expressions of this commitment;

- should affirm its commitment by communicating its determination to fight corruption internally and externally;

- should stipulate in the code of conduct that resorting to corruption is not one of the organisation's practices in its business dealings, relations with private and public sector partners or in its customer relations.

More specifically, top management should use indicators and the organisation's audit reports to ensure that the anti-corruption system is organised, effective and up to date.

2.2. Mainstreaming anti-corruption measures in policies and procedures

Anti-corruption measures should be integrated into all of the organisation's policies and procedures, including:

- human resources management procedures, making sure that compliance with ethical practices is incorporated into the recruitment and appointment process for all of the organisation's employees, especially, management personnel. Compliance should also be considered when setting annual objectives and conducting performance reviews. Managers' initiatives to promote the prevention and detection of corruption by their teams should be highlighted;

- within the whistleblowing system for reporting suspected or confirmed cases of corruption, by guaranteeing employees that whistleblowing or refusing to engage in non-compliant practices will not harm their career prospects, and that they will not be subject to retaliation, discrimination or disciplinary actions;

- within all other policies and procedures related to a process defined as high-risk by the corruption risk map.

2.3. Governance of the corruption prevention and detection programme

Governance of the corruption prevention and detection programme at the highest level of the organisation ensures the credibility of the action and top management's proactive approach.

Top management should appoint a compliance officer with responsibility for overseeing the deployment, implementation, evaluation and updating of the anti-corruption compliance programme, in close collaboration with the organisation's stakeholders. Top management should formally validate the risk management strategy implemented on the basis of the risk map and ensure that the chosen plan of action is carried out.

Top management also makes sure that the resources allocated for preventing and detecting corruption are adequate. For this purpose, top management should identify and organise the responsibilities of each person in the hierarchy to optimise the impact of the strategy.

2.4. Communication policy

The French Anti-Corruption Agency recommends that the organisation adopt an internal and external communication policy that is appropriate for its structure and its business activities.

The Agency recommends communicating with all of the employees and external partners about the organisation's policy for preventing and detecting corruption and the main thrusts of its compliance programme.

External communication about the main thrusts of the organisation's policy for fighting corruption will help to inhibit inappropriate internal and external requests and promote the development of best practices and a race to the top for ethical practices.

Finally, specific communication actions could be helpful for promoting training on corruption risks.

Anti-Corruption Code of Conduct

The Anti-Corruption Code of Conduct (no matter what the organisation decides to call it in practice) testifies to top management's decision to commit the organisation to preventing and detecting corruption. This code should be clear, unconditional and unequivocal.

It should set out the organisation's commitments and principles in this matter. It should define and illustrate the various types of behaviour to be barred as likely signs of corruption.

1. Contents of the Anti-Corruption Code of Conduct

The Anti-Corruption Code of Conduct should be initiated by the organisation's top management. It should set out the organisation's values and commitments with regard to preventing and detecting corruption. Top management's support for the Code will promote a culture of compliance, ethics and integrity.

The Code of Conduct provisions should deal with the types of behaviour the employees are likely to encounter as a result of the organisation's business activities. It should describe prohibited situations and behaviours. The description should be backed up with illustrations that are relevant for the organisation.

The Code of Conduct may refer to practical instructions (or "*process*", or "*procedure*", etc.) that define in detailed operational terms, based on risk mapping, the conduct required to manage high-risk situations.

The Code of Conduct should be more than just a collection of best practices; it should also prohibit practices that are inappropriate under the circumstances specific to the organisation. For this purpose, it should address gifts, invitations, facilitation payments, conflicts of interest, patronage and sponsorship and, where appropriate, lobbying.

The Code of Conduct should stipulate the disciplinary sanctions for prohibited behaviours and, more generally, behaviours that do not comply with the organisation's commitments and principles with regard to preventing and detecting corruption. If the disciplinary sanctions are set out in the employment regulations, the Code of Conduct may refer to such regulations.

The Code of Conduct should describe the internal whistle-blowing system for employees' disclosures of conduct or situations that infringe the Code of Conduct.

2. Scope of the Anti-Corruption Code of Conduct

The Code of Conduct should apply to all of the organisation's employees.

It should be applicable, with any necessary adaptations, wherever the organisation does business, including other countries and without prejudice to the enforcement of any more rigorous anti-corruption standards of another country.

3. Form and Dissemination of the Code of Conduct

The Code of Conduct should be a written document. It should be written in French, using simple and clear terms to ensure the adherence of all employees. It may be translated into one or more other languages so that it can be understood by employees from other countries.

The Code of Conduct should be disseminated within the organisation and incorporated into the training provided to the organisation's employees.

The Code of Conduct may also be part of a more broadly based "ethics" system that encompasses more than just fighting corruption, as long as its presentation remains perfectly comprehensible and it is incorporated into the employment regulations.

As a good governance tool, the Code of Conduct may be shared by all of the companies in a group, as long as this option does not undermine the effectiveness of the Code.

The Code of Conduct can also be used as a tool for external communication in dealings with customers, users, suppliers and, more generally, the organisation's partners.

4. The Code of Conduct and Employment Regulations

Insofar as the Code of Conduct is used to define the compliance required of employees, it should be incorporated into the employment regulations.

If the organisation is not required to adopt employment regulations, in France or in other countries, then the Code of Conduct should be given to employees or made accessible to them, using procedures to be defined by the organisation, as long as proof of dissemination or access can be provided. Dissemination or access should provide a complete and up to date version of the Code.

5. Updating the Anti-Corruption Code of Conduct

The Code of Conduct should be updated periodically, especially after any significant update of the risk map, as in the case of a reorganisation or a restructuring. For this purpose, the Code of Conduct should indicate the date it takes effect.

Internal Whistleblowing System

The internal whistleblowing system is a corollary of the Anti-Corruption Code of Conduct. As such, it gathers disclosures from employees about conduct or situations that do not comply with the Code and are likely to constitute corruption.

1. Objectives of the Internal Whistleblowing System

The internal whistleblowing system is the procedure that organisations implement to enable employees to disclose potentially non-compliant behaviours and situations to an anti-corruption officer, to eliminate such behaviours and situations and to impose sanctions where appropriate.

The internal whistleblowing system should be one part of an overall system for preventing and detecting corruption.

2. Operational Implementation of the Internal Whistleblowing System

The French Anti-Corruption Agency recommends that the internal whistleblowing system specify the following:

- the role of the whistleblower's superior, who should be able to guide and advise employees, unless the superior is the perpetrator of the non-compliant behaviour;
- the person assigned the function of receiving whistleblowers' reports within the organisation: the employer may outsource this function or assign it to a person within the organisation;
- the measures taken to ensure whistleblowers' anonymity, the confidentiality of the disclosures and the persons named in them, even when investigation and processing of disclosures require communication to third parties.
  If one or more persons are named, the organisation must be very vigilant when gathering evidence or documents, especially when the persons named in the whistleblower's disclosure can destroy compromising data or documents;
- the procedures for whistleblowers to provide any information or documents to back up their reports;
- procedures for communicating with the whistleblower;
- provisions for notifying the whistleblower immediately of receipt of the disclosure and the time needed to examine its admissibility. For this purpose, it should be stated that the acknowledgement of receipt does not mean the disclosure is admissible;
- the measures taken to notify the whistleblower of the end of the proceedings and, where appropriate, the persons targeted by the proceedings;
- if no action is taken, the provisions taken to destroy items on file that may be used to identify the whistleblower and the persons named in the disclosure within two months of the end of the investigation;
- if automated processing of disclosures is used, with the authorisation of the French Data Protection Authority (CNIL);
- where appropriate, the policy on processing anonymous reports: the processing requirements specified should be appropriate for the complexity of investigations involving anonymous whistleblowers. Furthermore, when possible, investigators should communicate with the anonymous whistleblower.

Organisations with a compliance department or officer may rely on their existing structures to consolidate the systems that are already in place.

The matters reported to top management through whistleblowers' disclosures should be used to update the risk map, while ensuring the confidentiality guaranteed by the system.

3. Possible Alignment with Legal Provisions Applying to Whistleblowers

The internal whistleblowing system should be distinct from the procedures implemented to ensure protection of whistleblowers under the terms of Articles 6 to 16 of the Transparency, Anti-Corruption and Economic Modernisation Act 2016-1691 of 9 December 2016[3], and from the whistleblowing mechanism for disclosing risks specified by Act 2017-399 of 27 March 2017 on the corporate duty of vigilance for parent companies and subcontracting companies.

Insofar as the internal whistleblowing system includes disclosures of risks covered by the abovementioned legislation, a single technical system for receiving such disclosures could be established in compliance with these provisions.

Under the circumstances, the legal rules on whistleblowers require care to protect their rights and strict confidentiality concerning their identity, as well as the matters disclosed and the persons named. Whistleblowing must also be possible for external and occasional collaborators.

If, when setting up a single technical system for receiving disclosures, organisations are unable to distinguish between disclosures under the different systems, the legal rules applying to whistleblowers may be extended to cover all disclosures.

3. *The appendix includes a summary of the legal provisions on whistleblowers*.

Appendix

Summary of Legal Provisions on Whistleblowers

Articles 6 to 15 of the Transparency, Anti-Corruption and Economic Modernisation Act 2016-1691 of 9 December 2016 stipulate the general status of whistleblowers.

However, these provisions are not applicable to matters, information or documents covered by national defence secrecy, medical confidentiality or attorney-client privilege.

1. Definition of Whistleblowers

Article 6 of the Act of 9 December 2016 stipulates "*a whistleblower is a natural person who reveals or reports disinterestedly and in good faith, a crime or an offence, a clear and serious violation of an international commitment duly ratified or approved by France, of a unilateral act by an international organisation pursuant to such a commitment, or of laws and regulations, or a serious threat or damage to public interest, of which he or she has personal knowledge*."

Under the law, the combination of five characteristics defines a whistleblower:

- the whistleblower is a natural person: a legal entity (e.g. association, professional body, etc.) cannot be deemed to be a whistleblower and is not covered by the provisions of the Act of 9 December 2016;

- the whistleblower has personal knowledge of the matters disclosed: the whistleblower is not reporting someone else's findings, he or she is reporting his or her personal findings, which could reasonably be thought to constitute the matters covered by Article 6 mentioned above;

- the whistleblower is disinterested: he or she will gain no advantage or reward for his or her disclosure. The support (e.g. from a trade union) that the whistleblower might seek if he or she feels under threat does not jeopardise the disinterested nature of the action;

- the whistleblower acts in good faith: at the time the whistleblower discloses the facts, these must have the appearance of corruption, so that the whistleblower cannot be accused after the fact of having sought to do harm to others.

Furthermore, a person making allegations that he or she knows are false cannot be deemed to be acting "*in good faith*" and is liable to prosecution for malicious denunciation under Article 226-10 of the French Criminal Code.

- the matters disclosed are serious: this criterion should be assessed under the terms of the Act, which stipulates a crime or an offence, a clear and serious violation of an international commitment made by France, or of an act by an international organisation pursuant to such a commitment, or a serious threat or damage to public interest. Corruption offenses meet this criterion.

2. Whistleblowing Procedures

2.1. Ordinary whistleblowing procedure

Even when a system for receiving whistleblowers' disclosures is in place, anyone wishing to disclose the matters referred to in Article 6 of the Act of 9 December 2016 must first disclose them to their direct or indirect superior or to a person designated by the employer.

Anyone may also submit their disclosure to the Rights Defender to be directed to the appropriate body.

If the person receiving the disclosure does not take action after a reasonable period, the whistleblower may take a second step and notify the judicial or administrative authorities, or professional bodies.

Disclosures concerning violations mentioned in Article 17 of the Act of 9 December 2016 or corruption may be submitted directly to the French Anti-Corruption Agency. Where appropriate, the Agency will refer the disclosures to the relevant Public Prosecutor, under the terms of Article 40 of the Criminal Procedure Code.

If none of the bodies contacted has dealt with the disclosure after three months, it may be made public.

2.2 2.1. Urgent whistleblowing procedure

In cases of serious and present danger or risk of irreversible harm, the disclosure of matters mentioned in Article 6 of the Act of 9 December 2016 may be submitted directly to the judicial or administrative authorities, or to professional bodies. It may also be made public.

3. Protection for Whistleblowers

The main protections are as follows:

- whistleblowers are not criminally liable if the criteria given in the definitions set out in Act 2016-1691 of 9 December 2016 are met, if the disclosure is "*necessary and proportionate to safeguard the interests concerned*" and if the disclosure complies with the whistleblowing procedures (Article 122-9 of the French Criminal Code);
- whistleblowers in the private sector, civil service and military cannot be dismissed, punished or discriminated against in any way for disclosing matters in compliance with the whistleblowing procedure (Article L 1132-3-3 of the Labour Code; Article 6 ter (A, 2) of Act 83-634 of 13 July 1983; Article L. 4122-4 (2) of the Defence Code).

Risk mapping

Risk mapping is an essential tool for monitoring corruption risks and constitutes the foundation for risk management strategy. Organisations use risk mapping to understand the factors that are likely to affect their activity and their competitiveness in order to protect themselves from the legal, human, economic and financial consequences of deficient vigilance.

Organisations use risk mapping to deepen their knowledge and strengthen control of corruption risks.

Risk mapping also helps ensure safer interaction with the ecosystem and a more secure business model, insofar as:

- it provides knowledge of the organisation's specific internal and external risks and of the managerial, operational and support processes[4] required for its activities;

- risk mapping requires identifying the roles and responsibilities of the players involved at every level of the organisation.

1. Corruption Risk Mapping, Definition and Objectives

Corruption risk mapping is the action of identifying, assessing, prioritising and managing corruption risks that are inherent in the organisation's activities.

Corruption risk mapping has two interrelated objectives:

- on the one hand, identifying, assessing, prioritising and managing corruption risks to ensure that the anticorruption compliance programme is effective and appropriate for the business models of the organisations concerned;

- on the other hand, informing top management and providing those responsible for compliance with the clear vision of risks needed to implement prevention and detection measures that are proportionate to the risks identified in the risk mapping exercise.

2. Charateristics of Corruption Risk Mapping

Risk mapping is:

- comprehensive in that it covers organisations' managerial, operational and support processes from "*end-to-end*". It identifies corruption risks with due consideration of the specific characteristics of each organisation: business sectors, geographical areas, stakeholders, business lines and processes.

Therefore risk mapping needs to involve the players controlling the processes at different levels of the hierarchy, from top management to teams on the ground;

- formalised meaning that it takes the form of a structured written document. It must be ready for immediate submission to officials from the French Anti-Corruption Agency;

4. For the purposes of these Recommendations, the notion of process encompasses all of the correlated tasks and interactions aimed at meeting managerial, operational and support needs.

- adaptable given the need to reassess risks periodically, especially each time a major element of the organisation changes. Updating the risk map should be part of an ongoing process that enables organisations to improve their risk management.

3. A Six-Step Method

Corruption risk mapping starts with an objective, structured and documented analysis of the organisation's exposure to corruption risks in the course of its activities. The description covers the impact of risks (seriousness) and the likelihood that they will occur (frequency), matters that are likely to increase risks (aggravating factors), and the responses given or to be given as part of an action plan.

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

1st step: clarifying roles and responsibilities for elaborating, implementing and updating the risk map.

Roles and responsibilities should be distributed as follows within organisations:

- top management should be solely responsible for the organisation's decision to undertake action to fight corruption risks. This responsibility cannot be delegated.

Top management's clear, unconditional and unequivocal commitment promotes a culture of compliance and transparency, which is essential for assessing risks. The corruption risk map per se can be presented at a meeting of a dedicated committee, for example. Top management validates the risk map and supports the risk management strategy based on the risk map.

Top management ensures that resources allocated to fighting corruption are proportionate to the risks. It ensures that the anti-corruption compliance team members have sufficient human and financial resources to perform their duties.

- the compliance officer should be appointed by top management. This function does not have to be performed by an entity that is dedicated solely for this purpose, as long as the designated person reports to top management and has an appropriate position in the hierarchy. Furthermore, this person must enjoy genuine functional independence vis-à-vis other departments and have the skills and means necessary to perform the compliance function.

The designated compliance officer oversees the deployment, implementation, evaluation and updating of the anti-corruption compliance programme, working closely with the organisation's stakeholders.

Top management should initiate the risk mapping exercise and provide the compliance officer with the means for implementing it. This officer oversees the elaboration of the risk map, by supporting the organisation's audit of business lines, functions and processes, its identification of the corruption risks incurred and its implementation of the appropriate prevention measures.

Once the risk map has been produced, the compliance officer should submit it to top management, which then validates the risk management strategy implemented on the basis of the risk map. Then top management should ensure that the chosen plan of action is implemented.

- those responsible for managerial, operational and support processes (e.g. sales manager, purchasing manager, etc.) should participate in the elaboration and updating of the risk map. They should report on the specific risks in their areas of responsibility so that probabilities, potential aggravating factors and risk ratings can be assessed.

- the risk manager should define the methodology for identifying, analysing and prioritising corruption risks. This manager should work closely with the compliance officer and report to top management on implementation of the risk management strategy.

- employees should contribute to the risk mapping exercise by reporting factors that are specific to their functions and to the risks incurred so that probabilities, potential aggravating factors and risk ratings can be assessed.

2nd step: identifying risks that are inherent in the organisations' activities

This step aims to establish the classification of risks that organisations incur in their activities.

This should not be a classification of theoretical risks that these organisations are exposed to, but a precise description of the actual situation that can be used to detail and document the specific risks they incur.

Consequently, surveying the risks inherent in an organisation's activities requires knowledge of the organisation and the roles within it, along with a detailed analysis of its processes.

Risk mapping exercises should, therefore, give due consideration to the action of third parties, insofar as this action may involve exposure to solicitations for corrupt purposes (risk factor). The organisation should also implement proportionate third-party due diligence to prevent the risk of external solicitations.

3rd step: assessing exposure to corruption risks

This step assesses the vulnerability of the organisation to each risk identified in the previous step. This step should identify the organisation's "*gross*" risk exposure resulting from its activities, before this exposure is adjusted for the prevention measures taken.

This vulnerability should be assessed using three indicators:

- an analysis of risk factors or sources: high-risk countries or business sectors, nature of the operations, new products, high-value contracts and/or very complex contracts, dealings with third parties, business pressure, weak internal controls, highly competitive environments, mergers and acquisitions, entering and exiting markets, asset disposals, new strategic partnerships, setting sales objectives, etc.;

- probabilities determined using the most comprehensive and appropriate information for the specific nature of the identified risk (e.g. past incidents);

- assessment of aggravating factors, by applying risk coefficients, for example.

To make the risk map as comprehensible as possible, we recommend including an appendix to explain methodology for computing "*gross*" risks and the definitions used. The risk identification and classification procedures used may also be included in an appendix to the risk map.

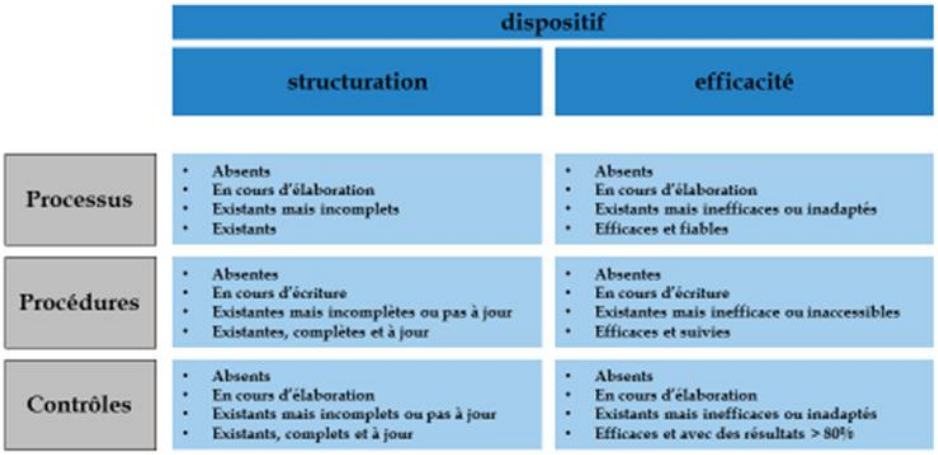
4th step: assessing the adequacy and effectiveness of the means for managing these risks

This step assesses effectiveness of the organisation's corruption risk management in order to compute the "*net*" or "*residual*" risk exposure incurred in its activities. This means adjusting the "*gross*" risk exposure in consideration of the prevention measures taken.

At this point in the risk mapping exercise, the effectiveness of existing prevention measures should be assessed. The assessment will depend on the structure of the systems in place and the outcome of their implementation.

To make the risk map as comprehensible as possible, we recommend including an appendix explaining the methodology for computing "*net*" or "*residual*" risks and the definitions used. The risk identification and classification procedures used may also be included in an appendix to the risk map.

Example of a table for assessing prevention measures:



	Systems	
	Structure	Effectiveness
Processes	• Absent • Under development • In place, but incomplete • In place	• Absent • Under development • In place, but ineffective or inappropriate • Effective and reliable
Procedures	• Absent • Under development • In place, but incomplete or out of date • In place, complete and up to date	• Absent • Under development • In place, but ineffective or inaccessible • Effective and enforced
Controls	• Absent • Under development • In place, but incomplete or out of date • In place, complete and up to date	• Absent • Under development • In place, but ineffective or inappropriate • Effective with > 80% success rate

5th step: prioritising and addressing "*net*" or "*residual*" risks

Once the "*net*" or "*residual*" corruption risks have been determined, they should be prioritised, distinguishing between risks for which the level of internal control is deemed to provide reasonable assurance that the risk is under control and risks management would like to manage better and provide stronger internal control.

Once this tolerance limit has been set and defined in the appended procedure, it is a matter of determining which measures to implement as part of the risk management strategy to remedy the

shortcomings of the prevention system, thereby limiting the probability of occurrence and of failure to anticipate aggravating factors.

The action plan should be developed on this basis. The timetable and procedures for implementation of the action plan, along with the related monitoring and accountability procedures should be the responsibility of specifically designated players.

6th step: officialising and updating the risk map

The risk map should be a structured written document. The findings should be presented in summary form. It should be noted that the form of the risk map facilitates its use as a tool to manage corruption risks.

Organisations may choose to organise their documentation by business line, by process, by entity or by geographical zone. The documentation should come with an appendix that describes the risk mapping procedure and the classification methodology for corruption risks.

The need for an update of the risk map should be assessed once a year. In any event, the corruption risk map should be updated to account for any changes in activities. The following events call for a review of the risk map: change in the business model, new processes or changes to processes, changes that affect the organisation, such as organisational changes or mergers-acquisitions, or any significant changes in the regulatory or economic environment.

Third-Party Due Diligence Procedures

In the course of their business in a given sector, organisations have dealings with various third parties, such as customers, suppliers, agents and contractors. If they fail to conduct due diligence with regard to the integrity of the third parties that they deal with, they may find themselves more or less directly implicated in corruption.

The risks they incur are legal, commercial and financial. Their image and reputation could also be harmed. Therefore they should conduct due diligence to ensure that third parties provide sufficient assurance of their integrity.

This takes the form of assessments based on the corruption risk map to rate the specific risk incurred in current or planned dealings with a given third party. These assessments are referred to as "due diligence". This exercise does not preclude other prudential measures that the organisations may take, such as specific contract clauses adapted to the third party's business sector.

1. Due Diligence Definition

Due diligence should be defined on the basis of the risk map. It consists of gathering information and documents about a third party so as to identify (or update) and assess the corruption risk exposure that an organisation incurs in initiating or continuing a relationship with a third party.

Due diligence should be conducted before the official start of the relationship. In the course of the relationship, due diligence should be updated periodically, with a predefined frequency appropriate to the level of risk, or whenever events occur that have an impact or a potential impact on the level of risk. Such events include mergers and acquisitions, amendments to articles of association or a change of management.

2. Due Diligence Objectives

Due diligence serves two purposes:

- on the one hand, it informs the decision to start, continue or end a business relationship;
- on the other hand, it enhances the effectiveness of measures to prevent and detect corruption implemented on the basis of the risk map and third-party due diligence.

3. Scope of Due Diligence: the Third Parties Concerned

Due diligence focuses on the third parties with which the organisation has or is about to start a relationship, with the priority on third parties identified as presenting corruption risks in the risk map.

The scope of due diligence should be broader than the priorities[5] set in Article 17-II-4 of the Transparency, Anti-Corruption and Economic Modernisation Act 2016-1691 of 9 December 2016.

5. Limited to customers, lead suppliers and agents.

Due diligence requires risk mapping of all third parties, according to their nature, status and size, in order to identify those that should be the object of due diligence that is proportionate to the level of risk.

Setting up a database of third parties[6], or even an information system, could facilitate processing and management.

The due diligence recommended here is distinct from the customer due diligence required of entities defined in Article L. 561-2 of the Monetary and Financial Code relating to the fight against money laundering and terrorist financing (Article L.561-1 et seq. of the Monetary and Financial Code), even though the two are compatible.

4. Due Diligence Procedures

- **Participants**

There should be three levels of due diligence participants within organisations:

- line managers, who conduct due diligence and are accountable for it, should gather the information and documents concerning the third parties that they are or will be dealing with. These managers should submit their preliminary findings. These findings may constitute the final decision in low-risk cases;
- the compliance officer (or any other designated manager) should provide expertise and advice to the line managers. This officer should provide line managers with support in the highest-risk cases;
- top management should make the final decision in the highest-risk cases notified by the line managers.

Coordination between the different levels should avoid the risks of operational errors, conflicts of interest and fraud.

As necessary, organisations may outsource third-party due diligence, particularly when they do not have the means to obtain the information and documents required, or when the third parties concerned reside and/or do business in a country where the organisation is not represented.

- **Helpful Information and Documents**

The organisation should determine the relevant information and documents based on the corruption risk map, its business model and its interests. For example, due diligence may include:

- gathering information from the organisation's internal documents;
- gathering information from open sources, public documents or publicly available information, such as articles in the press, financial statements and court records;
- checking to see if the third party or its beneficial owners[7], managers or directors are on the lists of individuals and entities subject to sanctions (including lists of individuals and entities banned from government contracts financed by development banks and the list of individuals and entities subject to financial and international sanctions published by economy and finance ministries);

6. In compliance with the principles and procedures stipulated in the Act 78-17 of 6 January 1978 relating to data processing, computer records and freedom.

7. Meaning the natural persons who directly or indirectly control the third party.

- checking to see if the beneficial owners, managers, or directors of third parties include any politically exposed persons;
- gathering information from commercial databases;
- gathering information and documents from the third parties by such means as questionnaires, interviews, audits, or internal authorisation or certification processes.

5. Due Diligence Content

Organisations should ensure that the use of third parties is justified and meets a real need, especially in the case of service providers or agents. They should also provide the reasons that led to the choice of a specific third party rather than a competitor. The fact that a customer recommends or requires the use of a given third-party is a danger signal, for example.

The following points should also be verified, in compliance with the applicable regulations, particularly regulations dealing with data protection, fighting money laundering and competition.

- **Identity**

Organisations should ascertain the main elements of third parties' identity: name, corporate name, legal structure, incorporation date, number of employees, turnover, registered capital, business sector(s), qualifications (particularly in the case of agents and service providers) and location(s).

- **Ownership**

Organisations should ascertain the first and last names of the main shareholders and the beneficial owners, meaning the individuals and entities that directly or indirectly own more than 25% of the shares or voting rights or, failing that, the individual or entity that directs and manages undertakings for collective investment (Articles R 561-1 and R 561-2 of the Monetary and Financial Code).

- **Country Risk**

As part of the risk mapping exercise, the corruption risk specific to different countries should be rated based on the organisation's experiences. In addition, this risk may be assessed using:

- the list of countries subject to financial and international sanctions published by economy and finance ministries;
- OECD monitoring reports on implementation of the Convention on Combating Bribery of Foreign Officials in International Business Transactions in the signatory countries;
- the Corruption Perceptions Index (CPI) published annually by the NGO, *Transparency International.*

When conducting due diligence, country risk is determined by the level of risk for countries of residence, as well as the countries where the third parties and their businesses are registered. For example, the fact that a third party is registered in a non-cooperative jurisdiction or a country without equivalent legislation may be defined as a risk factor when rating the third-party risk.

- **Business Sector**

Organisations should establish a procedure for rating the level of corruption risk by business sector. The sector ratings should be updated periodically, depending on the corruption risk map and the organisations' own business experiences. In addition, organisations may use the list

published by the NGO, *Transparency International* (Transparency International Bribes Payer Index Report 2011, latest edition).

When conducting due diligence, the sector risk is determined by the level of risk in the business sectors where the third party earns its revenue.

- **Expertise**

Organisations should ensure that the thirds parties (agents or service providers) have the necessary experience, qualifications and skills to perform their tasks.

For this purpose, organisations may ask third parties to provide the necessary references, depending on the data already obtained (incorporation date, start-up date, etc.)

A lack of qualifications or experience may be seen as an aggravating factor when rating third party risk. Organisations should also ensure that the compensation is consistent with the level of expertise and the services provided.

- **Integrity and Reputation**

Organisations should ascertain whether third parties, their managers, main shareholders and beneficial owners have been the subject of adverse information, allegations, prosecution or convictions for any offences and, more particularly, corruption offenses. The level of third-party risk should be adjusted for the findings of such investigations.

- **Compliance**

Organisations should ascertain whether third parties have developed anti-corruption compliance systems. The fact that third parties do not mention or document the implementation of such a system may be seen as an aggravating factor when rating third-party risk.

- **Cooperation**

The third parties' behaviour should be considered when assessing risks: a third party's refusal or reluctance to provide the requested information or documents may be seen as a risk factor when rating the third-party risk.

- **Nature and Purpose of the Relationship**

Organisations should define the requirements for execution of the contract precisely, since the level of third-party risk will vary depending on the nature and the purpose of the contractual relationship.

Some types of relationships involve acute levels of corruption risk, such as third parties engaged to help the organisation win contracts: on the one hand, the organisation may encourage the third party to engage in non-compliant activities in order to circumvent its own anti-corruption compliance programme and, on the other hand, the third party may engage in such activities on its own initiative, without informing the organisation.

- **Other Players**

Organisations may do business in ecosystems involving several players, without necessarily being linked to each of them (e.g. supply chains). In such cases, organisations should ensure that the third parties they deal with do their own third-party due diligence.

Organisations should also assess the level of third-party risk associated with the distribution channel used and/or the use of an agent.

Generally speaking, the level of third-party risks varies, according to the nature of the other players and their own levels of risk.

- **Dealings with Government Officials and Politically Exposed Persons (PEPs)**

Dealings between the public and private sectors present a high corruption risk. Organisations should identify the dealings that third parties may have with government officials, noting their first and last names, especially when they are politically exposed persons[8].

The fact that third parties include politically exposed persons constitutes a risk factor to be considered when assessing the level of third-party risk.

- **Financial Considerations**

A long-lasting or high-value financial relationship may constitute a risk factor to be considered when assessing the level of third-party risk.

The currency used is also a factor to be considered, in view of the extraterritorial enforcement of some countries' anti-corruption legislation.

- **Compensation Procedures**

The compensation amounts for suppliers, service providers and agents should be consistent with the nature and scale of the goods and services sold by third parties and in line with market prices. If an inconsistency is found, the due diligence should be suspended until a reasonable explanation is provided.

Commission payments for winning contracts are a risk factor to be considered when assessing the level of third-party risk.

- **Payment Flows and Procedures**

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 a non-cooperative jurisdiction).

Organisations should also ensure that the requested payment procedures are consistent with usual practices. Risk factors to be considered when assessing the level of third-party risk include cash payments, cross-border payments or payments to other parties than the third-party concerned or payments made for non-itemised invoices.

6. Assessing the Level of Third-Party Risk

The assessment should be determined in two consecutive steps:

- an assessment (or rating) based on objective and quantifiable criteria (sanctions, business sector, incorporation date, etc.);
- consideration of qualitative criteria requiring analysis or judgment (aggravating factors, cooperation, etc.)

The level of risks assessed in the first step may be revised upward or downward in consideration of the qualitative criteria.

Ultimately, the third-parties are classified by level of risk (e.g. low risk, moderate risk, high risk).

7. Conclusions

Once the assessment of the risk level is complete, the decision should be made to:

- approve the relationship – with or without qualifications;
- end or not start the relationship;
- defer the decision (pending further assessment, for example).

8. *Meaning natural persons who perform or have performed important public functions in their own country, in another country or in an international organisation.*

The persons who make the decision 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 level of third-party risk (see 4 above).

If the due diligence does not reveal any risk factors, it does not guarantee a totally risk-free relationship with the third party. On the other hand, the identification of risk factors does not rule out a relationship, but it should incite the organisation to take appropriate measures to prevent and detect corruption.

7.1. Corruption Risk Prevention Measures

Measures to prevent and detect corruption should be adapted to the specific environment of each organisation, which means it is up to organisations to define the measures they deem consistent with their business model.

For this purpose, organisations may consider one or more of the following options:

- notifying the third party of their anti-corruption programme by providing a copy of the code of conduct, for example;
- providing corruption risk training or awareness-raising for the third party;
- requiring the third party to provide a written commitment to fight corruption.
  For this purpose, contracts deemed to be risky might include anti-corruption clauses. Such clauses make it possible to terminate the contract in the event of a lapse of integrity;
- requiring the third party to verify the integrity of its sub-contractors in order to secure the supply chain.

7.2. Monitoring Dealings with Third Parties

Dealings with third parties should be monitored to prevent and detect corruption.

Contracts should include specific provisions describing the services rendered by the organisation or the third party, as well as the compensation amounts and the payment procedures.

For this purpose, organisations must have comprehensive oversight of the payments received from or made to third parties so that they can ensure that the compensation and payment procedures comply with the contract provisions. The financial staff should alert the compliance officer or any other designated person when unusual payment procedures are requested (e.g. cash payments, or a change in the location of a bank account to a non-cooperative jurisdiction).

The process of renewing contracts should be used to ensure that third parties have complied with their anti-corruption commitments throughout the previous contract term.

7.3. Reviewing and Updating Third-Party Due Diligence

Due diligence processes should be repeated periodically, depending on the third parties' risk classifications. For this purpose, a due diligence review date should be set when starting the relationship.

Significant changes in third parties' circumstances, such as a merger or acquisition, should give rise to fresh due diligence, alongside the review process.

A simple update of qualitative criteria is acceptable if an organisation receives information about a third party that does not affect the level of risk in the course of the relationship.

8. Auditing the Third-Party Due Diligence Process

Auditing the third-party due diligence process involves three lines of defence:

- a "*first-level*" control conducted by line staff, aimed at ensuring due diligence is complete and consistent;
- a "*second-level*" control, conducted by the compliance officer or another designated person, to verify proper execution of the first-line audit;
- a "*third-level*" control conducted by the internal audit function to ensure that the third-party due diligence system complies with the organisation's requirements and is fully implemented and kept up to date.

9. Third-Party Due Diligence System Indicators

A system for monitoring the third-party due diligence system should be established. The monitoring should include:

- indicators relating to due diligence work completed;
- indicators relating to reviews to track compliance with the frequency of reviews of third-party due diligence;
- the findings of the first-level and second-lelvel controls;
- indicators for priority reviews, in accordance with a remedial plan for overdue or noncompliant due diligence revealed by the first-level and second-level controls.

All of these indicators and findings may be submitted to line management and the compliance officer or any other designated person as appropriate to their purpose.

10. Third-Party Due Diligence Record Retention

All of the third-party due diligence records and amendments to them should be retained for five years after the end of the business relationship (or the date of an occasional operation).

Accounting Control Procedures To Prevent And Detect Corruption

Accounting records are an assessment tool containing information about an organisation's operations and its intangible, physical and financial assets. Organisations prepare, classify, restate and aggregate their accounts to produce statements that provide a truthful representation of their operations.

Accounting control procedures are an important safeguarding tool that help organisations manage risk in general, and corruption risk in particular. Because they play an important role in preventing and detecting corruption, they should form part and parcel of an organisation's risk management strategy.

1. What Are Accounting Control Procedures?

Accounting control involves a set of documented, structured, permanent procedures, set by the top management team, to monitor how an organisation processes its financial information and to ensure proper financial and asset stewardship.

2. What Purpose Do Accounting Controls Serve?

Organisations use accounting control procedures to:

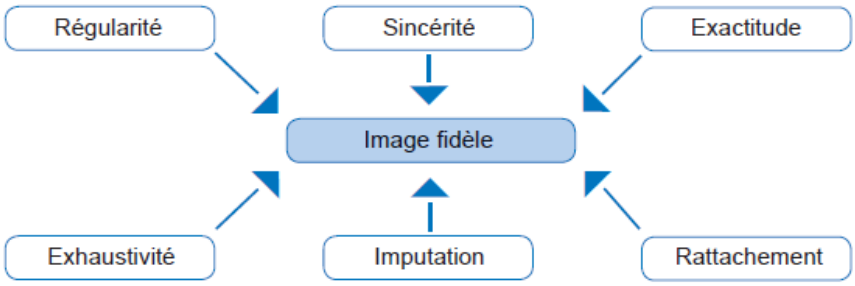
- safeguard their assets and cash resources (for example, making sure transactions are secure), by checking that their operations are well-managed, effective and exhaustive and that allocated resources are properly used (encompassing operational, financial and compliance risk);
- ensure that their books and accounts are not used to conceal acts of corruption, in order to comply with the Transparency, Anti-Corruption and Economic Modernisation Act 2016-1691 of 9 December 2016.

These procedures provide reasonable assurance that accounting information is produced to a high standard, and that an organisation's records provide a regular,[9] sincere[10] and faithful[11] picture of its accounting and financial situation.

Accounting control procedures ensure that an organisation prepares reliable information about its financial situation and assets, and about how these are managed.

9 . The principle of regularity states that an organisation's financial information should be prepared in a manner consistent with accounting principles and rules as prescribed by law.
10 . The principle of sincerity states that an organisation's financial information should reflect, in good faith, the reality of its financial situation to the best knowledge of the persons responsible for preparing the information.
11 . Faithfulness implies that an organisation's accounting records should accurately reflect its operations, the results of these operations, and its financial situation and assets.

The diagram below summarises the aims of these procedures:



Accordingly, organisations do not need to bring in new accounting procedures to ensure that their books and accounts are not used to conceal acts of corruption. Instead, they should consider concealment of corruption as one of the many risks that can arise when accounting records are not prepared regularly, sincerely and faithfully. Officials tasked with checking accounting records for foul play need to be made aware of this risk and educated about the importance of preventing and detecting corruption.

3. The Relationship between Accounting Controls and Audits

Accounting control procedures can include controls, audits, or both:

- controls are a set of documented, permanent internal procedures, employed by management at all levels of an organisation, to manage the risks inherent in its operations and to help ensure that the financial information it presents is faithful;
- audits are independent assessments intended to check whether the organisation is managing its operations properly, to advise on improvements, and to ensure that control procedures are sufficiently robust.

As such, accounting controls and audits are two separate, complementary procedures.

4. How Accounting Controls Are Performed

Accounting controls can be carried out in one of two ways:

- internally, by the organisation's accounting and finance department or by another, designated specialist entity (such as a shared services centre or management control unit);
- externally, by a designated outside entity.

Regardless of whether the controls are performed internally or externally, organisations are advised to adopt the "three lines of defence" model.

4.1 First level control

First level control typically involves those persons responsible for preparing and approving journal entries, who check that the entries are properly documented with supporting evidence (especially manual entries).

Ideally, risky journal entries should be checked and approved by another employee (i.e. not the person who made the entry) to guard against the dangers of self-checking.

In some cases, organisations may find it useful to introduce a threshold below which employees are able to cross-check each other's entries. Any entry above this threshold, meanwhile, will

need to be approved by the employee's line manager or, alternatively, referred to the second level control.

4.2 Second level control

Second level control exists to maintain high standards in the organisation's accounting system and to inform risk mapping. Checks are performed at various points throughout the year, independently of the persons involved in the first line of defence.

The purpose of this control is to ensure that the first level control is functioning correctly, and that accounting control procedures are working as they should. Where sample checks are used, the samples should be representative of the risks inherent in the organisation's accounting system (for example, manual entries, level of authority and segregation of duties).

Once the second level controls are complete, a summary report is drawn up indicating any irregularities uncovered and how they should be addressed.

4.3 Third level control

The third level control, also known as internal audit, is a process of ongoing assessment to determine whether accounting control procedures are effective.

Targeted audits of all accounting control procedures are scheduled at regular intervals, to check that they meet the organisation's requirements, are carried out properly and are regularly updated.

This control looks in particular at the following aspects:

- whether accounting control procedures are properly governed and adequately resourced;
- how the checks performed at the first and second levels are devised and whether they are properly applied;
- whether accounting controls give due consideration to corruption risk.

The organisation is at liberty to decide whether accounting control procedures are conducted internally, by an external entity, or a combination of the two. Whatever model is adopted, these procedures must be applied at all levels of the organisation. If the general control process excludes certain entities, by virtue of the group or legal entity's structure, organisations are advised to bring in separate controls for these entities that are suited to the nature of their operations.

An external auditor could be tasked with performing accounting controls to coincide with the statutory audits provided for in article L.823-9 of the French Commercial Code.

It is important to make clear, however, that this option is entirely separate from the duty incumbent on public limited companies, limited partnerships and limited companies to appoint a statutory auditor.[12]

Article L.823-9 of the French Commercial Code states that "the statutory auditors certify, justifying their assessments, that the annual financial statements are prepared regularly and sincerely, and give a faithful representation of the results of operations during the year and of the person's or entity's financial position and assets at the end of the financial year."

The statutory auditor's principal task is to certify the organisation's financial statements, issuing a certification report that indicates whether:

12 . This obligation only applies to companies if they exceed certain thresholds, depending on their legal form.

- the accounts are prepared regularly and in accordance with France's National Accounting Code;
- the accounts are sincere (prepared honestly and in good faith);
- the information provided is a faithful representation of the organisation's situation (principle of prudence, financial representation of reality).

Statutory auditors are tasked with helping organisations avoid potential problems down the line. So, as part of their investigations, they play a role in preventing and detecting corruption. Moreover, they are duty-bound to report any criminal acts they uncover during their work – including evidence of corruption – to the public prosecutor.

5. What Accounting Controls Entail

Accounting controls have a number of different aims – for example, checking that an organisation's accounting records give a true picture of reality, that they are prepared in accordance with the law and internal procedures, and that the amounts and transactions shown are proportionate, and determining who sent and received payments.

Organisations should therefore check who has access to the accounting system, and make sure that permissions are assigned in a manner consistent with the segregation-of-duties principle.

For these reasons, the accounting system should:

- make a clear distinction between manual[13] and automatic entries;
- identify the employee and department that made and approved each entry;
- be capable of retaining reversed entries;
- produce entry lists/journals showing all manual entries made per day/per department;
- have a permission denial feature (for example, if entries do not balance or a user tries to delete an entry).

The organisation's accounting record control policy should also target those operations that it considers especially risky, as determined by its risk mapping.

For example, an organisation might decide to target:

- operations such as donations and bequests, sponsorship and patronage payments, commission and fees, entertainment and marketing expenses, and gifts and hospitality;
- atypical transactions (such as suspense accounts);
- one-off or high-risk operations (such as acquisitions);
- operations involving third-party intermediaries (such as agents or consultants);
- financial or material flows to high-risk accounts or third parties.

13 . All journal entries must be accompanied by supporting documentation, bearing a date and duly approved, and must include a clear description of the nature of the operation, along with references explaining the treatment rationale, if any.

Corruption Risk Training

A robust, appropriately designed internal training system is an effective way to embed a culture of integrity across an organisation. It helps spread the message about top management's pledge to stamp out corruption, brings employees on board, and creates a common body of knowledge across all staff exposed to corruption risk.

While corruption risk training should be geared towards managers and employees with the greatest exposure, it is nevertheless useful to raise awareness of the issues throughout an organisation's workforce.

It might also be beneficial to raise awareness of corruption prevention and detection among board members and directors, especially when there is a change of personnel at the head of the organisation.

1. Who Should Receive Training?

The head of human resources should work with the compliance officer (or any other designated manager) to identify which managers and other employees are most exposed to corruption risk (i.e. those people responsible for high-risk processes), as determined by the organisation's risk mapping. For example, these individuals might be managers and other employees who work with exposed third parties (for example, salespeople or buyers).

As well as pinpointing high-priority targets, organisations should devise and deploy a broader training and awareness plan so that, over time, all employees are trained to prevent and detect corruption, regardless of their degree of exposure.

2. What Should the Training Entail?

Organisations will need to devise separate training programmes – one for managers and other employees who are most exposed to corruption risk, and another for other employee categories.

The programme content will vary according to the types of risk encountered, individuals' duties, and the regions in which the organisation operates, and should be reviewed regularly to reflect changes in the organisation's risk mapping.

2.1. Training for most exposed managers and other employees

These programmes are designed so that most exposed managers and other employees assimilate the organisation's anti-corruption system and are actively engaged in detecting and preventing corruption.

To achieve this outcome, trainees will need to understand:

- the processes and risks involved;
- what checks they need to perform to mitigate these risks;
- how to deal with an inappropriate request;
- what disciplinary sanctions they will face if they engage in non-compliant practices.

The training covers the following topics:

- top management's commitment and the organisation's code of conduct;
- corruption in general, why it is an issue, and what forms it can take;
- what the law says about corruption and the penalties that apply;
- the anti-corruption compliance framework;
- how to deal with corruption when it happens (including individual roles and responsibilities).

In addition, the organisation should deliver targeted training on the specific high-risk activities singled out in its risk mapping (such as public procurement).

Employees in this category should also receive training on how to handle whistleblowing reports (articles 6-16 of the Transparency, Anti-Corruption and Economic Modernisation Act 2016-1691 of 9 December 2016, how to forward these reports to the relevant department for further investigation, and the duties incumbent on line managers under the organisation's whistleblowing system.

2.2. Training for other employee categories

These programmes might cover aspects such as:

- top management's position on corruption and the organisation's code of conduct;
- corruption in general, why it is an issue, what forms it can take, and the penalties that apply;
- how to deal with corruption when it happens (including individual roles and responsibilities).

3. How Is the Training Delivered?

The organisation may deliver the training itself, or bring in an external body to do so under its authority.

The training should be delivered in an appropriate format, either in-person or as e-learning modules, and in a language that the target audience can understand.

Ideally, training for most exposed managers and employees should be delivered in person, drawing on case studies and practical examples that are meaningful to the target audience and aligned with the organisation's corruption risk exposures. Other representatives of the organisation could be brought in to talk about their experiences, and to discuss their reactions and thoughts on the matter.

E-learning modules could be used to supplement the in-person sessions or to raise awareness of the issues among employees who are less exposed to corruption risk.

Managers should ensure that all team-members have completed anti-corruption training and understood the content of the programme. Completion of the training could form part of the employee review process.

4. Training Oversight

A training oversight process can help organisations maintain high standards and ensure that training provision is effective. Again, the three levels of controlshould be carried out:

- first level control: managers make sure all staff-members have completed anti-corruption training and understood the content of the programme;

- second level control: the head of compliance (or any other designated manager) ensures that the first line of defence is functioning correctly, and that the anti-corruption training programme is working as it should (in particular, that the right module types and formats are being delivered at the prescribed frequency);
- third level control: internal audit checks whether the training has been delivered as prescribed and whether the expected outcomes have been achieved.

5. Training Indicators

Organisations are advised to develop a set of indicators to track and measure training provision. Typical indicators could include target population coverage rate or completion rate.

Where training is outsourced, the external provider must provide the head of compliance (or any other designated manager) with the delivery timetable and programme content. The compliance officer should also monitor delivery and track the corresponding indicators.

Internal Monitoring and Assessment System

Organisations should implement an internal monitoring and assessment system to make sure corruption prevention and detection measures – informed by its corruption risk mapping – are appropriate and effective.

This system has four aims:

- to check that corruption prevention and detection measures are being implemented, and whether they are working;[14]
- to detect and investigate any shortcomings in implementation;
- to issue recommendations and other corrective measures, if any, to enhance anti-corruption compliance programme performance;
- to detect corruption, if any.

A system of this type is designed to make sure the organisation has a fully functioning anti-corruption compliance programme that aligns with its identified risks, and to detect any areas where the system can be improved.

1. First level control

The organisation's corruption detection and prevention measures should align with its identified risks, as informed by its risk mapping. These measures form part and parcel of internal processes and are implemented day to day by employees across the organisation.

The first level control exists to ensure that all operational or support process tasks are carried out in accordance with internal procedures. Checks at this level may be performed by operational or support staff (self-checking or cross-checking) or by line managers (line management checks), who will need to know what to look out for and what checks are required. First-level controls must therefore be mentioned explicitly in the organisation's procedures.

Any issues encountered at this stage should be reported to the head of compliance (or another designated manager), who will then investigate the issue and determine what corrective action to take.

2. Second level control

The purpose of the second level control is to ensure that the first level control is functioning correctly, and that the corruption prevention and detection system as a whole is working as it should.

The head of compliance (or another designated manager) should draw up a plan, covering the corruption prevention and detection system in its entirety, outlining what checks are required at this level of control. The plan should include a brief description of the key aspects of each check, the system and risk category covered, and the anticipated dates of completion (if the checks have already been performed, the plan should include the completion date and outcomes of each check).

For each check, the plan should indicate:

14 . *Article 17-II of the Transparency, Anti-Corruption and Economic Modernisation Act 2016-1691 of 9 December 2016 states that the companies and public establishments of an industrial and commercial nature (EPICs) mentioned in article 17-I must implement an "internal monitoring and assessment system of the measures implemented".*

- its scope;
- the person(s) responsible;
- the methodology (how the check is performed, what supporting documentation is sought, and what analysis and assessment methods are used);
- its frequency;
- how the outcomes and corrective action, if any, are shared.

Once each check is complete, it should be documented and all associated records kept. The French Anti-corruption Agency's investigatory powers give it the authority to demand that organisations produce these records.

3. Third level control

The third level control, also known as internal audit, is a process of ongoing assessment to determine whether corruption prevention and detection measures are effective. The anti-corruption system is audited to check that it meets the organisation's requirements, is properly implemented and is regularly updated.

3.1. Audit plan

Organisations should draw up a documented audit plan, informed by risk mapping. The plan should identify all functions involved in the monitoring system, since the auditors will require input from the named individuals and functions during their investigations. The organisation may wish to consider the following points in particular:

- whether the corruption prevention and detection system is properly governed and adequately resourced;
- how its corruption risk map and code of conduct were produced, and how these documents are applied;
- the key rules that shaped the third-party risk assessment system, and how these rules are applied;
- how the internal whistleblowing system is designed, and how it works in practice.

3.2. Internal auditors

Internal auditors are tasked with objectively and independently analysing how anti-corruption measures are implemented, identifying any shortcomings, and suggesting appropriate ways to make the organisation's compliance system more effective.

As such, it is essential that internal auditors have the authority they need to carry out their work, as well as the competencies and resources to implement the annual audit plan. Internal auditors should be given access to the organisation's documentation and locations as required, and the power to talk directly to employees.

Organisations may also bring in external auditors if they so wish.

3.3. Internal audit process

The organisation's size and risk exposures will determine how audits are carried out. Organisations may opt to audit their subsidiaries where corruption risk exposure so demands. All internal monitoring and assessment audits must be documented, and all associated records kept.

Any shortcomings in implementation (including those reported by the first and second levels of control) must be investigated, so that the root cause can be identified and appropriate corrective action taken. In some cases, employees may not be sufficiently familiar with corruption prevention and detection measures, or the measures may be overly complex, restrictive, unworkable or unsuitable. In other cases, shortcomings may arise because of poor organisation,

ineffective management, under-resourcing or deficient communication, or because staff are not properly trained.

Audits can also detect emerging risks, implying that the organisation needs to update its risk mapping and revise its processes.

Where internal audits uncover corruption exposure mechanisms or evidence that corruption has occurred, the auditors must report the matter to the head of compliance (or any other designated manager) and to the top management team, so that an internal investigation can be launched. If the investigation proves conclusive, the top management team must uphold its commitment and report the matter to the competent authorities (see recommendation on top management's commitment to prevent and detect corruption).

3.4. Audit report

Once the internal audit process is complete, the auditors should draft a comprehensive written report outlining any shortcomings, along with corrective action and guidelines. The report should be formally shared with the top management team.

As well as making certain that the report's guidelines are implemented, the top management team should play its part in embedding an internal audit culture across the organisation, by making sure the internal monitoring and assessment system is adequately resourced and by encouraging feedback. This, in turn, can help to ensure that employees:

- treat corruption with the seriousness it deserves;
- are aware of best practice and good conduct;
- are more likely to detect risks when they arise;
- have a firmer grasp of corruption prevention and detection measures;
- are encouraged to report malpractice via the internal whistleblowing system.

Clarifications for the Public Sector

The Agency's Guidelines are France's official anti-corruption policy framework. They apply across French territory and are designed to help France uphold its international commitments on preventing corruption.

The section that follows provides additional clarification on these guidelines for the public sector, where required. The Agency's general guidelines and principles are published on its website.

All public sector entities – whether governed by public law or private law – are tasked with delivering public services, irrespective of their legal status and staff employment arrangements.

For the purpose of this document, the term "public sector entities" means:

- central government (central administrations, devolved central government administrations, departments with national scope, independent administrative authorities, etc.);

- local governements and groups of local governements;

- public establishments (other than EPICs with more than 500 employees and turnover in excess of €100 million, which are covered by article 17 of French Act 2016-1691 of 9 December 2016);

- public interest groups;

- publicly owned companies (including local publicly owned companies and semi-public companies);

- non-profit organisations with a public service role.

The Agency's Guidelines – a unified, indivisible policy framework – should be applied by all public sector entities, in a manner consistent with each organisation's size and risk exposures.

1. Top management's Commitment to Implement an Anti-Corruption System

Each public sector entity's senior leadership team should:

- publicly pledge to treat all morally or ethically inappropriate conduct with zero tolerance;[15]
- lead by example on integrity and probity through their own words and deeds (senior managers who accept gifts – other than those with symbolic value – or misuse departmental resources set a bad example and could encourage other staff to engage in inappropriate conduct);
- encourage and acknowledge ethical conduct among staff;
- explicitly make preventing and detecting corruption a top priority within the organisation;

15 . *Article 25 of French Act 83-634 of 13 July 1983 on the rights and obligations of civil servants states that "civil servants shall fulfil their duties with dignity, impartiality, integrity and probity […]. Heads of department shall ensure that these principles are upheld in the departments under their authority. Heads of department may, after consulting employee representatives, devise a set of department-specific ethical principles that apply to all officials under their authority."*

- introduce an internal anti-corruption system that reflects the organisation's risk exposures and unique characteristics, if any;
- remain on their guard at all times, decide what evidence of suspicious conduct could amount to corruption risk within their organisation, and use their judgement when deciding whether to investigate veiled references and rumours originating from outside the organisation, as well as anonymous tip-offs;
- consistently and proportionately use the disciplinary sanctions available to them (as per the French Civil Service Code[16] and/or the French Labour Code) as a dissuasive measure (failure to discipline employees for inappropriate conduct can give the impression that corruption is permitted within an organisation).

2. Code of Conduct

An organisation's code of conduct is a standalone document. It is entirely separate from other, existing frameworks, such as internal charters of ethics (where they exist), the Charter for Local Elected Representatives (created by article 2 of French Act 2015-366 of 31 March 2015 to help them carry out their duties, and codified in article L.1111-1-1 of the French Local Authority Code), or French Act 2016-483 of 20 April 2016 on the ethical duties, rights and obligations of civil servants.

A code of conduct should contain a series of binding rules, with disciplinary sanctions for employees who breach these rules.

It should not simply restate the general ethical principles that apply to the public sector. Instead, it should be a clear-cut document that addresses the risks identified in the organisation's risk mapping, translating general ethical principles into specific guidance and containing a set of rules on how local officials should conduct themselves in specific, everyday situations.

In particular, the code of conduct should:

- explain why it is important for public sector entities to prevent corruption;[17]
- provide hands-on examples of risky situations;
- explain how best to handle these situations when they occur (e.g. rejecting bribes outright when offered and reporting the matter to line management at appropriate level; bringing one or more colleagues along as witnesses in case of uncertainty; managing casework transparently and keeping work and private life entirely separate; stepping aside if a conflict of interest arises; and reporting breaches of the duty of probity, or procedural issues);
- define what is meant by conflicts of interest and explain how employees should step aside if a case involves them personally, or their ascendants, descendants, indirect relatives or acquaintances;
- make absolutely clear the circumstances under which a person may hold elected office and work as a public official at the same time;
- spell out the main warning signs, if applicable;
- state that elected representatives and public officials have a duty to declare conflicts of interest, and explain how to go about reporting them;
- address questions around gifts and hospitality (type, amount, frequency, source, etc.);

16 . *https://www.fonction-publique.gouv.fr/statut-general-des-fonctionnaires (in French)*

17 . *For example, these reasons could include (without being limited to) preventing: harm to institutional and civil service reputations; breaches of the principle of equal treatment of citizens; misuse of public funds; declining public service standards (delivery of sub-standard goods, works and services); and sub-optimal resource allocation.*

- provide guidance on secondary employment and other business interests.

3. Risk Mapping

Risk mapping methodology guidance is provided in the detailed recommendation on this subject.

Corruption risk mapping is about identifying, assessing and prioritising corruption risks inherent in an organisation's remit, activities and processes, so that these risks can be managed effectively.

Organisations are advised to engage in risk mapping.

In practice, risk mapping involves:

- identifying all internal processes, as well as external processes in which the organisation's representatives are involved, and describing these processes in detail;
- defining individual roles and responsibilities within each of these processes (for public officials, employees of public-law or private-law entities, or elected representatives);
- determining appropriate decision-making and internal control procedures for high-risk operations.

Risk mapping should be an exhaustive, detailed exercise, identifying all risks inherent in how the organisation operates and the functions it performs. Because it involves an end-to-end analysis of decision-making and action processes, it necessarily requires input from the department's officials and, where applicable, elected representatives. The risk map should be documented and available to view.

Risk mapping should encompass all circumstances in which public officials, employees of public-law or private-law entities, or elected representatives could offer or receive a benefit, of whatever nature, in the performance of their duties – in return for making, or failing to make, a given decision.

A risk map is a dynamic document that should be reviewed as often as is necessary to account for changes in the organisation's remit and procedures.

Organisations may opt to carry out risk mapping internally (e.g. with assistance from the audit or internal control department), or bring in outside expertise to assist with the task.

If the risk mapping process itself reveals evidence of corruption, managers may need to take immediate safeguarding measures. These might include:

- removing files and records for ongoing or closed cases;
- denying access to case files;
- locking offices, tightening security around departmental memos and reports, and limiting access to work resources (such as computers);
- reporting the matter to the criminal authorities if necessary.

In any event, all evidence of corruption should be recorded so that subsequent corrective action can be tracked.

Once the risk mapping process is complete, the organisation should take targeted action to mitigate the identified risks as far as possible. This could include:

- tightening security around procedures;
- introducing enhanced internal controls;
- reassigning individual officials, managers or elected representatives;

- limiting the number of people allowed to access computerised records;
- assessing the integrity of contractual and other partners;
- introducing stricter checks around contract award and implementation;
- introducing stricter checks around grant award and implementation.

4. Internal whistleblowing system

The recommendation on internal whistleblowing systems describes what purpose a system of this type serves and how to implement it in practice. It also summarises what the law says about whistleblowers (articles 6-15 of the Transparency, Anti-Corruption and Economic Modernisation Act 2016-1691 of 9 December 2016, and how the internal whistleblowing system relates to this legal framework.

This recommendation applies to public sector entities and to non-profit organisations.

French decree 2017-564 of 19 April 2017 on the procedures for handling whistleblowing reports provides the following protections for whistleblowers, with effect from 1 January 2018:

- central government bodies, departments with national competence and devolved central government departments: the whistleblowing system is created by order of the relevant minister(s), who may introduce a single system covering all departments and public sector entities under their authority, after securing the consent of each entity's duly empowered body;
- non-state legal entities governed by public law, municipalities with a population in excess of 10,000 people, *départements*, regions and their public entities, and government-funded inter-municipal cooperation institutions with tax-levying powers containing at least one municipality with a population in excess of 10,000 people: the relevant whistleblowing requirements are indicated in article 8-III of French Act 2016-1691 of 9 December 2016, and entities may opt to join forces under a single system;
- semi-public companies and local publicly owned companies: these entities are subject to the same rules as legal entities governed by private law.

Organisations must publicise their whistleblowing procedures by any suitable means (e.g. via a circular, poster, printed document or email, or on their website, if any), such that they are made available to all permanent employees and officials, as well as to external and occasional staff.

5. Third-Party Due Diligence Procedures

For public sector entities, the term "third party" refers to any party outside the organisation, including contract bidders and winners, organisations applying for or receiving grants, and job applicants.

Public sector entities may have particularly complex relationships with third parties that use consulting firms to advise on the operation under assessment or that work with subcontractors, as well as with third parties applying for or securing premises or the right to occupy state or private property (among others).

Informed by their risk mapping, entities perform a series of checks (commonly known as "due diligence") to ascertain the level of risk inherent in the existing or potential relationship with a third party.

In some cases, entities may be obliged to perform certain checks by law. For example, French ordinance 2015-899 of 23 July 2015 on public procurement requires entities to check that candidates have not been convicted (with no further right of appeal) of an offence that precludes them from bidding for public contracts. Yet internal assessment procedures should not be limited to what is required by law.

Public sector entities have the freedom to build anti-corruption guidelines or requirements into their schedule of obligations, to help ensure that all parties conduct themselves with integrity before the schedule is adopted, and during performance of their obligations. Moreover, introducing compulsory requirements can provide a legal basis for subsequent sanctions in event of a breach.

6. Internal Monitoring and Assessment Systems

The recommendation on internal controls applies in its entirety to public sector entities.

Moreover, when enforcing the rules on internal monitoring and assessment that apply explicitly to them, public sector entities should consider the specific requirements around preventing corruption and breaches of the duty of honesty:

- French decree 2011-775 of 28 June 2011 on internal audit in the administration states that each ministry must have a system, "appropriate for its remit and the structure of its departments, for managing risk in the management of public policy under its charge" (such systems can make a meaningful contribution to preventing corruption, even though no specific mention is made of this in the decree).
- Other public sector entities are at liberty to introduce internal control and audit systems to prevent and manage risk, if they so wish.

  These systems are designed to capture any activities that could go against the entity's duty of probity, covering both internal activities, and dealings with peripheral entities (non-profit organisations managing service delivery, local semi-public companies, local publicly owned companies, low-income housing associations) and third parties (suppliers, service providers, etc.).

  Authorities such as metropolitan areas, regions, *départements*, urban district communities, large town and city councils and other heavily resourced public sector entities are strongly advised to introduce systems of this type.

The Agency's recommendation on internal accounting controls also applies to public entities, even if they are subject to separate accounting rules.

Under the segregation of duties between the authorising officer and the accounting officer, the authorising officer commits, settles and orders both incoming payments and expenditures, keeping a record of the transactions in an administrative accounting inventory. The corresponding processes must therefore be subject to stringent internal controls.

Controls of this type are designed to give the authorising officer reasonable assurance that the accounting information is reliable and that the accounts were prepared in accordance with the law (and, in particular, that the accounting decision-making chain precludes the possibility of recording irregular transactions). In any event, the authorising officer should seek out substantive evidence that the corresponding services were actually delivered, rather than relying solely on supporting evidence of the expenditure.

Importantly, however, this segregation-of-duties model should not relieve the accounting officer of his or her duty to perform the usual checks (even when the entity employs line management expenditure checks or simplified joint checks by the accounting and authorising officers). Entities may find it useful to organise the invoice processing department's work in a way that streamlines joint checking tasks, all the while ensuring that checks remain exhaustive.

7. Corruption Risk Training

Public sector entities will need to provide anti-corruption training for the following individuals, regardless of their status:

- people who are considered most exposed to corruption risk because of their position and duties, as identified in the entity's risk mapping (highest-priority targets);
- people with less exposed positions and duties;
- people in supervisory, audit or control roles;
- new recruits (inadequate initial training is a common complaint across the public sector, as many younger employees are apparently unaware of the basic ethical principles that apply to public office and lack the common sense to handle inappropriate requests in the right manner);
- new elected representatives (who often find themselves elected to office without suitable training);
- all people dealing with third parties (in the long run).

Ideally, entities should have an anti-corruption training plan with different delivery types and formats (continuing professional development, special annual sessions, in-person training, e-learning and self-study materials).

Entities could work with outside partners to support training delivery, such as accredited training providers, professional organisations, and Network of Public Service Schools (RESP) members offering targeted modules on this subject.