RÉPUBLIQUE FRANÇAISE

Liberté
Égalité
Fraternité

AFA
Agence Française Anticorruption

The AFA's guidelines for companies subject to Article 17 of the Transparency, Anticorruption and Economic Modernisation Act 2016-1691 of 9 December 2016

Official Journal of the French Republic of 12 January 2021

The guidelines

- **Purpose**

The guidelines, along with the Act, the implementing decrees and the guides published on the AFA's website, constitute the **French anticorruption policy framework**. They offer a methodologic tool to support the development of an anticorruption programme.

- **Legal force**

The guidelines are not legally binding, but the AFA refers to them when carrying out its advisory and audit missions (as of July 2021)

A company stating that it has followed these guidelines shall benefit from a prima facie presumption of compliance

A company that choses another method must demonstrate that its choices comply with the requirements of the Act if deficiencies are found during an audit.

The guidelines

Principle of proportionality

Companies should adapt these guidelines in accordance with their risk profile, which depends on different criteria such as :

- Size
- Organisation
- Location
- Governance
- Third-party categories
- Industries

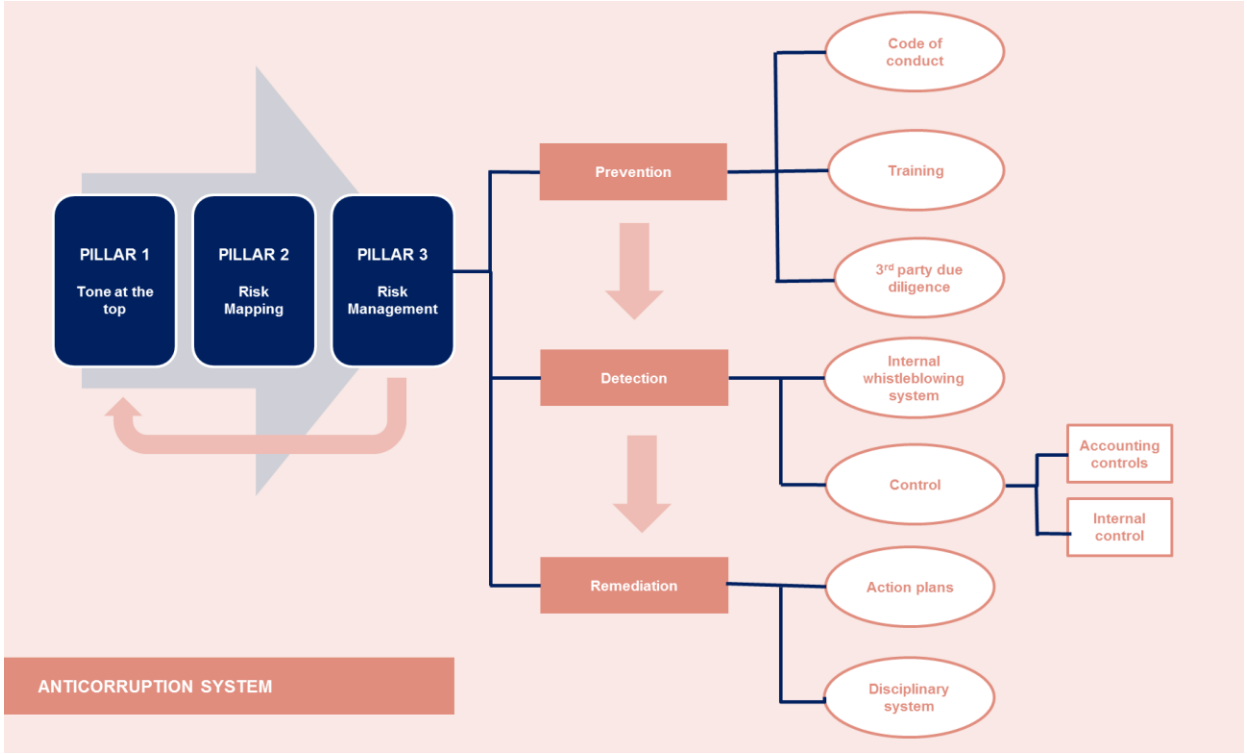
Recommended scope of intervention

The anticorruption programme covers **corruption and influence peddling** and, to the extent possible:
- Prior offenses: **forgery, misuse of corporate assets**
- Consecutive offenses: **concealment** or **laundering of the proceeds of these offenses**

The scope of the corporate anticorruption programme should include all directly and indirectly controlled entities.

Anticorruption programme

Overview



This programme includes the elements defined by the Law (Article 17-II), presenting them through a systemic approach, in accordance with the best practices identified in the field of anticorruption.

First pillar: Tone at the top (1/6)

Definition

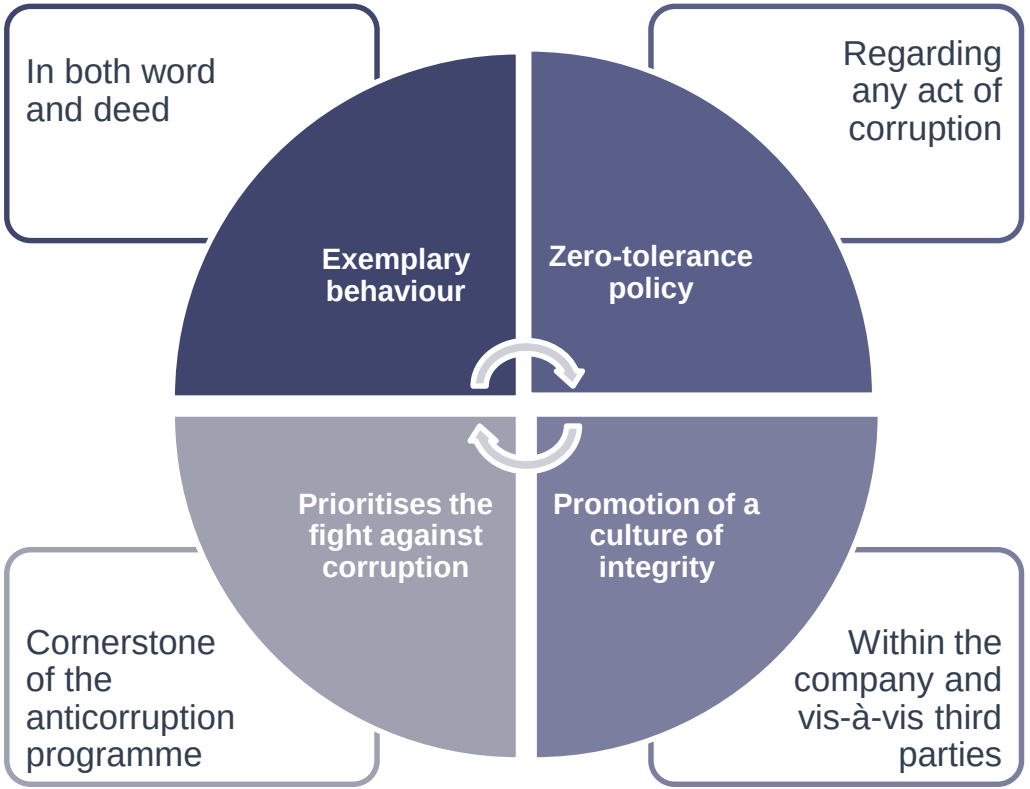
Entity	Top management under Article 17-I
A company or a group of companies	Chairs, CEOs, Company's legal representative
Government-funded industrial and commercial institutions (EPIC), e.g. State-Owned Entities (SOE)	Chairs and CEOs
Limited liability companies governed by article L.225-57 of the Commercial Code	Management board members

It is recommended that the anticorruption programme and its updates be periodically presented to the members of the board and directors or other governing or supervisory bodies, as they shall have all necessary information to ensure that the company complies with article 17 of the Act (§95).

First pillar: Tone at the top (2/6)

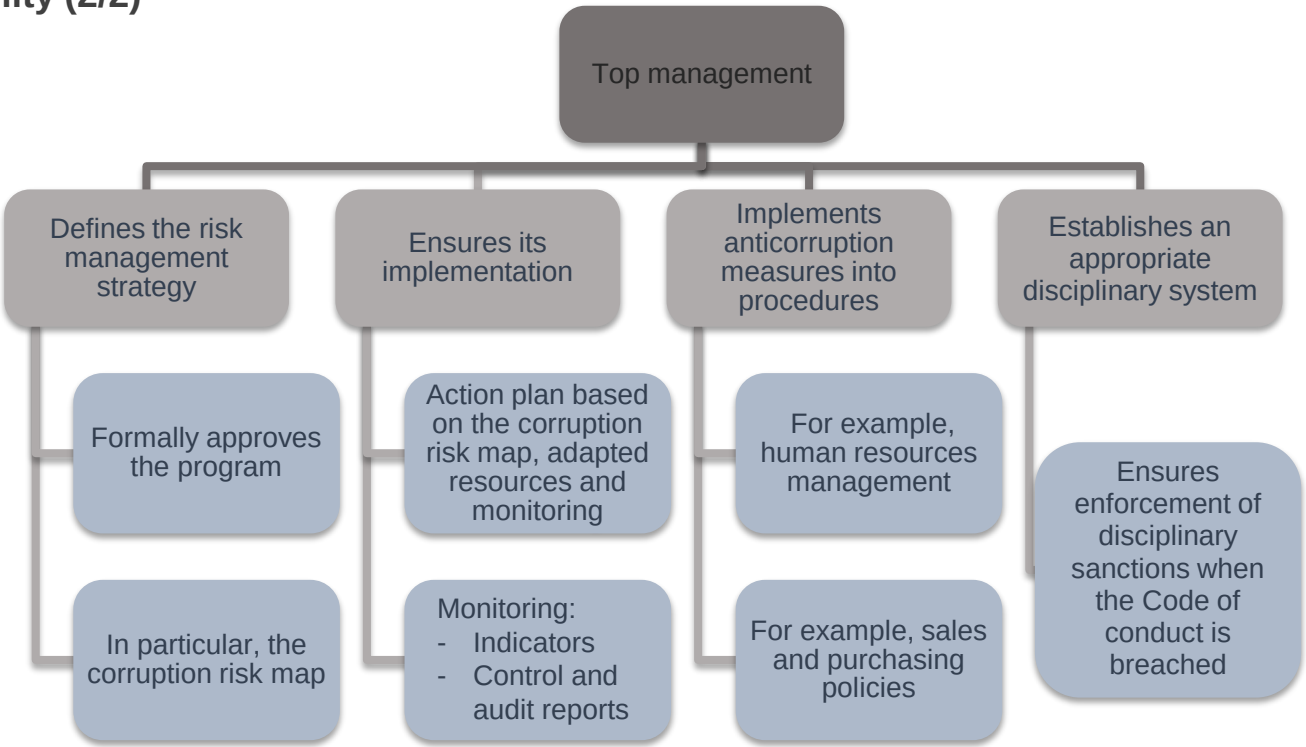
Responsibility (1/2)

Chair and CEO are legally liable for implementing an effective anticorruption programme which may, when appropriate, be operationally delegated to an anticorruption compliance officer.



First pillar: Tone at the top (3/6)

Responsibility (2/2)



First pillar: Tone at the top (4/6)

Resources dedicated to the compliance function

- An anticorruption compliance team
- Possible use of external consultants or service providers, where appropriate
- Implementation of tools (3rd-party due-diligence platform, internal whistleblowing systems, etc.)
- Management of anticorruption training
- Production of periodic reports and assessments
- Appropriate communication policy on the anticorruption program
  - **In-house**: frequent and broad-based, covering in particular the Code of conduct, anticorruption training and the internal whistleblowing system
  - **External**: to external partners via appropriate means (confidentiality)

First pillar: Tone at the top (5/6)

The compliance officer (1/2)

- **Reporting to top management**

Top management ensures that the compliance officer at any time :
- **has access to any information** useful for the performance of their tasks, providing a true and fair view of the company's activity;
- **is independent** from the company's other functions and the capacity to have a real influence on these other functions (independence does not imply the absence of supervision; the compliance officer reports on their activity to senior management);
- **has access to Top management** to ensure voice and support, as well as easy access to the board of directors.

- **Skills**

Demonstrated ability to operate cross-functionnaly

Clear understanding of applicable anticorruption regulations

Good command of risk management techniques

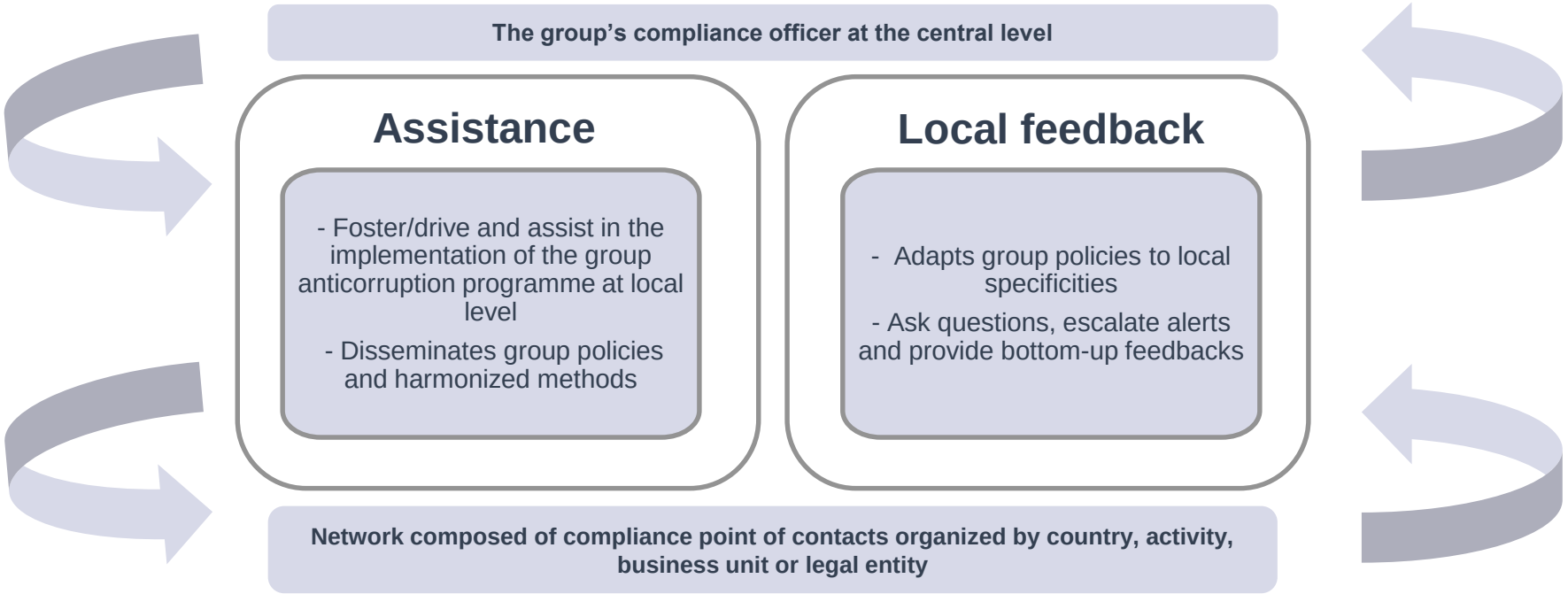
- **Appointment**

It is recommended that the compliance officer's appointment is announced to the entire staff by the Top management and their mission defined in an engagement letter detailing responsibilities and other relevant information (reporting, positioning vis-à-vis other company functions and compliance domains, allocated resources both human, financial and technical).

First pillar: Tone at the top (6/6)

The Compliance officer (2/2)

Organisation of a group compliance function



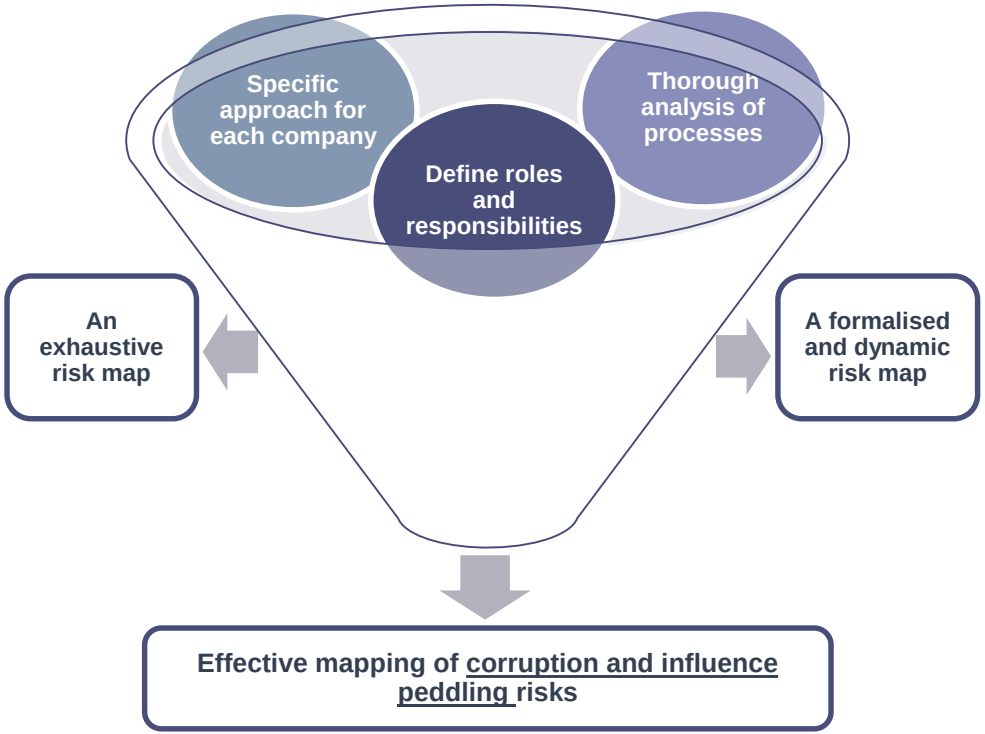
Second pillar: Corruption risk mapping (1/7)

Objectives

ALL PROCESSES
- Operational
- Managerial
- Support

ALL RISKS
- Activities
- Locations
- Regulations
- Third parties
- Internal organisation, etc.

THE WHOLE SCOPE
- Controlled companies
- Monitoring of implementation
- Global vision



FORMALISED
- Methods of development
- Risk management measures
- Roles and responsibilities

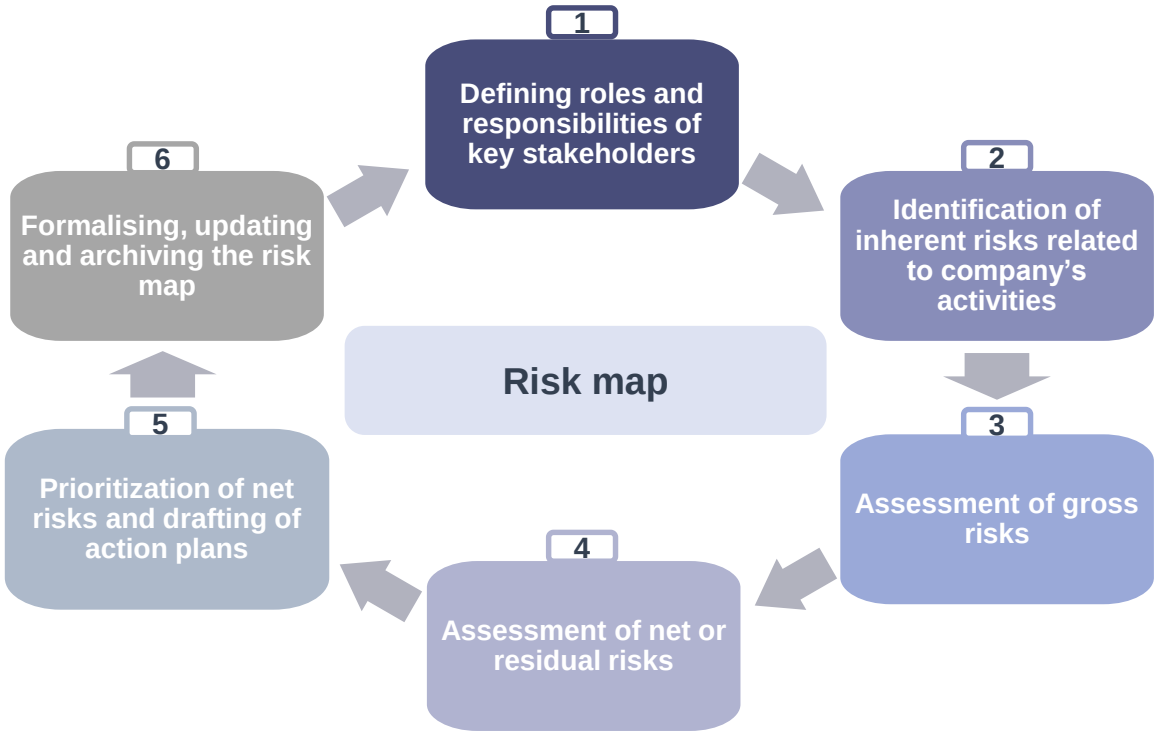
ORGANISED
- At the choice of the company (by activity, entity or geographies…)

RISK STEERING TOOL
- Facilitates audits of the programme, especially in case of administrative or judicial actions.

DYNAMIC
- Periodic reassessment of risks, particularly whenever a significant changes occur within the company

Second pillar: Corruption risk mapping (2/7)

Risk-mapping: a recommended 6-steps method



Similar risk-mapping exercises already conducted by the Company for others risks can be leveraged to map corruption risks.

Second pillar: Corruption risk mapping (3/7)

The different steps for establishing a risk map

✓ Step 1: Defining roles and responsibilities

Top management	- promotes the risk mapping exercise and provides the compliance officer with the necessary resources to conduct it; - approves risk management strategy based on the risk-mapping and ensures that related action plans are drafted and implemented.
Compliance officer	- coordinates the risk mapping exercise, guiding stakeholders in the identification of processes and related corruption risks, in the prioritization of these risks and in the definition and implementation of mitigating action plans; - responsible for drawing up the corruption risk map and submits each risk map update and action plan monitoring report to appropriate governing bodies for approval.
Process owners	- managerial, operational, accounting and other support process owners each contribute to the risk-mapping exercise and its update in their area of responsibility; - responsible for identifying risks that are specific to their activities in accordance with the company's anticorruption procedures.
Risk manager	- contributes to define the used for identifying, analysing, prioritizing and managing corruption risks.
Staff	- contributes to the mapping exercise by reporting on factors specific to their functions and the risks incurred in order to take appropriate steps to identify, assess and prioritize risks; - all staff, including executives and directors.

Second pillar: Corruption risk mapping (4/7)

✓ **Step 2: Identifying inherent risks in the company's activities**

- **Process identification**

Process identification	Discussions on each process	To list the risk scenarios
Based on the company's activities	Workshops, interviews, questionnaires (encourage free expression, draft and archive a written summary)	These scenarios are specific to the company
No pre-determined list of processes at risk	Staff from all hierarchical levels, selected based on their operational command of the processes	A list of risks in advance is just a starting point for discussions

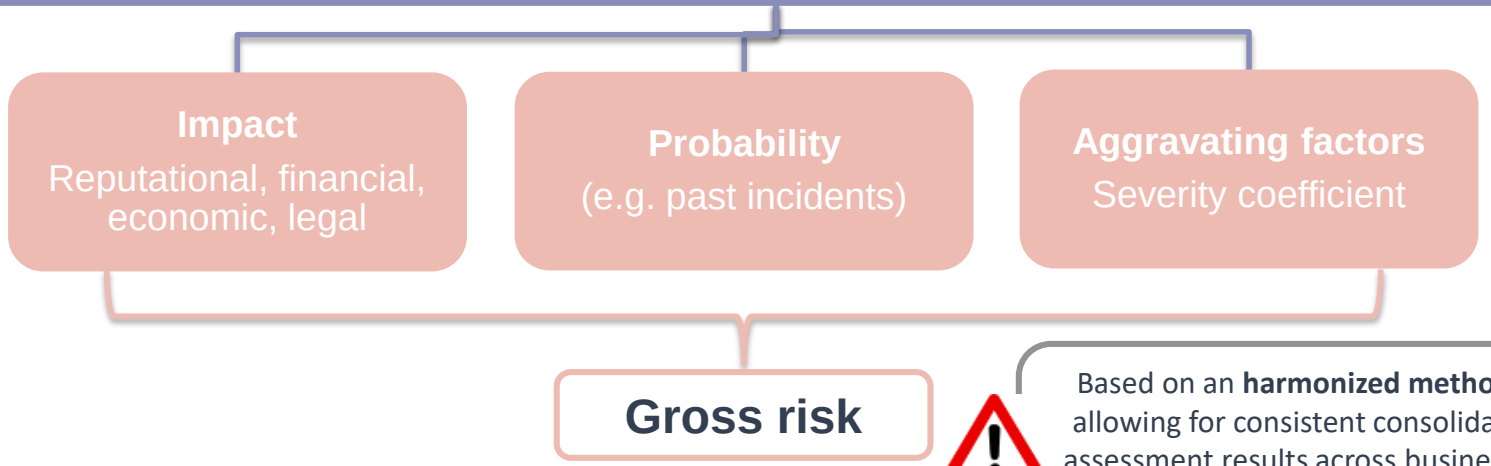
- **Risk factors that are specific to the company:**

- Geographies where the company operates
- Industries
- Strategic operations
- Third-party categories
- Length of the sales cycle
- Payment terms and conditions
- Past incidents involving the company
- Court decisions

Second pillar: Corruption risk mapping (5/7)

✓ **Step 3: Assessing gross risks**

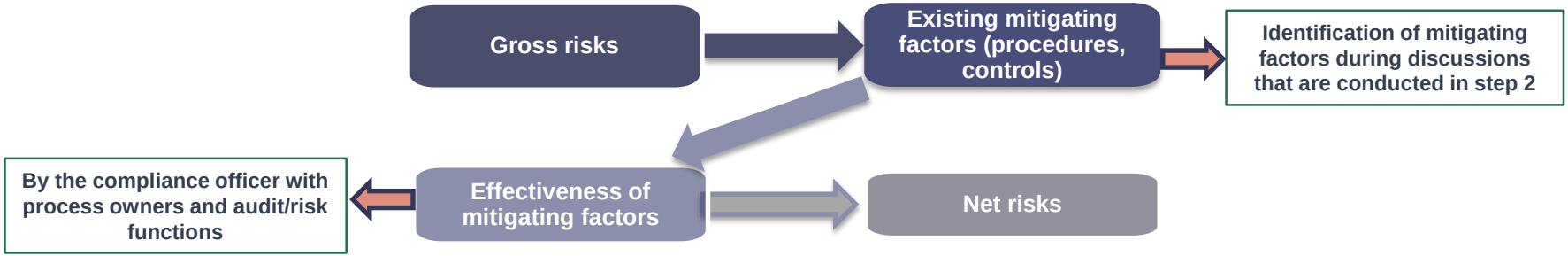
Objective: assess the company's vulnerability to each risk scenario, on the basis of a uniform methodology



Based on an **harmonized methodology** allowing for consistent consolidation of assessment results across business lines, legal entities and geographies in scope.

Second pillar: Corruption risk mapping (6/7)

✓ **Step 4: Assessment of net or residual risks**



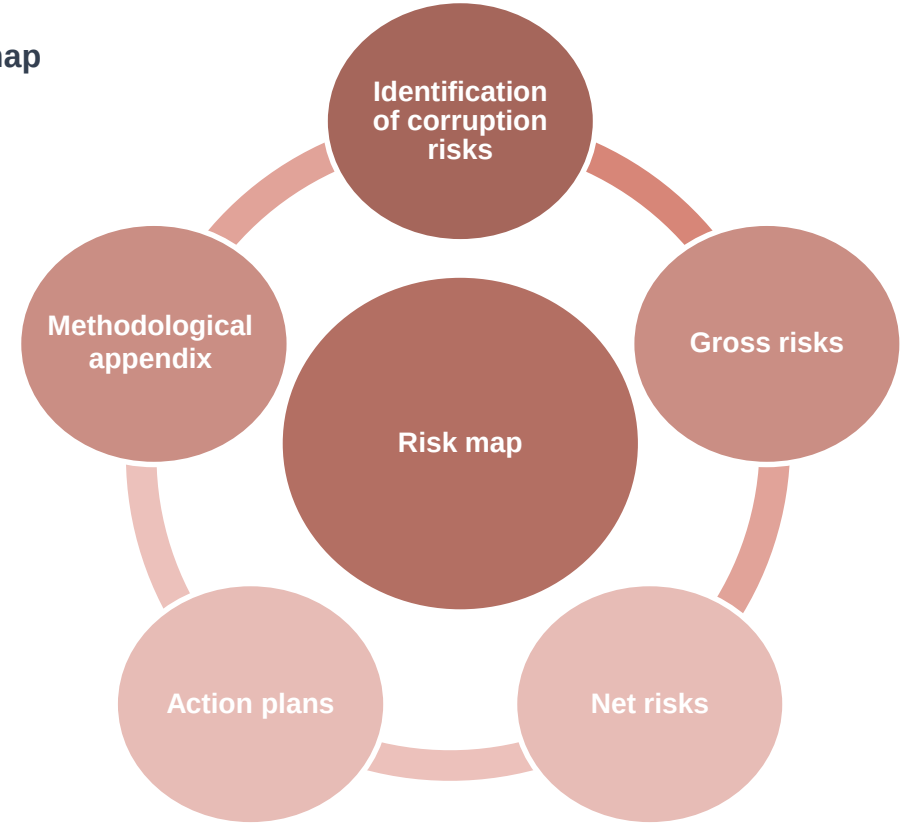
✓ **Step 5: Net or residual risk prioritization and preparation of action plans**

Second pillar: Corruption risk mapping (7/7)

✓ **Step 6: Formalising, updating and archiving the risk map**

The need to update the risk-mapping is assessed each year.

Retaining the following elements can be useful to assess the effective implementation of the risk mapping exercise:
- Records of discussions with staff (notes, written summaries);
- Method for calculating “gross” risks, and the definitions used;
- Method for calculating “net” or “residual” risks, and the retained definitions;
- Procedures for identifying and categorising risks;
- The different versions of risk maps submitted to appropriate governing bodies approval and the related approved action plans;
- Minutes of the project committee.



Third pillar: Risk management

Risk prevention: Code of conduct (1/3)

○ Definition and scope

Document that is an expression of senior management's commitment:
- recapitulates **the company's commitments and principles** regarding corruption prevention and detection;
- defines and illustrates behaviors that constitute a violation of the Code of conduct.

- The Code of conduct is **applicable to and binding for all company staff members**.
- The Code of conduct is **applicable everywhere the company operates, including other countries**. It can be adapted as needed to local specificities and the nature of activities.
- Other **staff (temporary workers, service providers, etc.) subject to internal regulations** must comply with the code.
- The Code may be **communicated to third parties** in a form which respects confidentiality obligations or by inclusion of a contractual provision.

○ Drafting and approval process

The Code of conduct is jointly drafted by the **compliance officer and qualified company staff**.

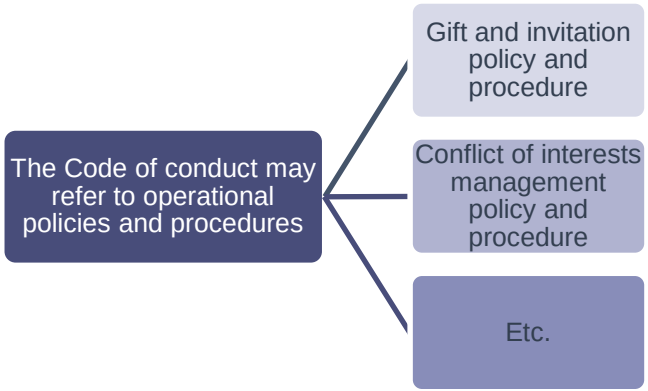
It is **approved by appropriate governing bodies**, which endorse the document, for instance by signing the foreword.

Top management promote the Code of conduct and abide by its principles. Tone at the top is key for the proper appropriation and correct application of its provisions by staff members.

Third pillar: Risk management

Risk prevention: Code of conduct (2/3)

Articulation and reference to other compliance documentation



All of these documents must be consistent with each other, clearly and understandably stated and accessible to all staff members.

Internal regulations – disciplinary regime

- The Code of conduct is included in corporate regulations.
- If the company is not required by law to adopt internal regulations in France or abroad, the **Code of conduct is provided to staff or made available to them** following procedures defined and retained by the company.

Ethics programme

The Code of conduct may also be incorporated into an “ethics” programme (such as a charter of ethics) with a wider scope**, provided that its presentation remains perfectly understandable**.

Third pillar: Risk management

Risk prevention: Code of conduct (3/3)

Content

- Code violations
- Relevant illustrations of actual cases
- May deal with gifts and invitations, conflict of interest, sponsorship and patronage...
- Internal whistleblowing system
- Disciplinary sanctions
- Designated function that will answer staff members' questions (e.g. compliance department)

The Code of conduct is written in **clear, straightforward and unequivocal terms**. It may be **translated into several languages** when necessary.

The opportunity to update the Code of conduct is periodically examined, in particular after completion of a **risk-mapping update**. To this end, it mentions an effective date.

Third pillar: Risk management

Risk prevention: Awareness and training (1/3)

Objectives

TRAINING

- **Mandatory** for managers and staff at risk
- Goal: provide knowledge, necessary skills and information to perform prevention and detection activities.
- The training programme should:
  - Be consistent with the other elements of the anticorruption programme;
  - Address the specific risk exposures of each category of personnel.

AWARENESS

- **Recommended** for all personnel
- Goal: provide information and raise awareness
- Awareness actions may focus on:
- The Code of conduct;
- Corruption in general, issues, types and incurred sanctions, whether disciplinary or criminal;
- Conduct to be adopted when confronted with corruption and individual roles and responsibilities;
- The internal whistleblowing system.

Third pillar: Risk management

Risk prevention: Awareness and training (2/3)

Mandatory training (1/2)

Improve understanding of:

- Processes and related risks;
- Corruption offenses ;
- Required due-diligence and measures to be taken to mitigate these risks;
- Conduct to be adopted when confronted with inappropriate solicitations ;
- Incurred disciplinary sanctions in the event of non-compliant practices.

For who?

Managers and staff who are **most at risk**, as identified during the risk-mapping exercise:

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

Content:

- Corruption in general, issues and types;
- Applicable legal requirements and the related sanctions;
- The anticorruption compliance programme;
- Conduct to be adopted when confronted with corruption, individual roles and responsibilities;
- The internal whistleblowing system.

- The content is **adapted to the company risk profile, *i.e.* its activities and the locations where it operates.**
- **Specific topics** are addressed, depending on the job positions of the participants.
- The content is **regularly updated** consistently with the **risk map updates**.

Third pillar: Risk management

Risk prevention: Awareness and training (3/3)

Compulsory training (2/2)

WHEN

- During the onboarding process.
- Throughout the course of their employment.

HOW

- Case studies and scenarios adapted to each audience and suited to the risks identified in the risk map.
- Sharing operational experience about corruption prevention and detection.
- Simulation exercises to favour ownership of the rules in everyday work.

FOLLOW-UP

- Developments of tools, such as tests, to check that participants have properly understood the training courses.
- Such tests could be performed by the end of the training course or some time after its completion to ensure that its content has been understood.

The compliance officer must:

- be notified of training schedules and content;
- monitor the deployment of the programme and the related indicators.

Indicators are set up to monitor the training programme and could include:

- Percentage of target audience trained;
- Number of training hours (including in the case of outsourced training).

Third pillar: Risk management

Risk prevention: Third-party due diligence (1/5)

For whom and why?

Mandatory: customers, direct suppliers and intermediaries

Recommended: other categories of third parties with which the company has or intends to initiate relationships, such as acquisition targets, or sponsorship and patronage recipients

To decide whether to **enter or not into a relationship with a third party**, maintain a relationship or end it.

Anticorruption third-party due diligence are **distinct** from anti-money laundering and counter-financing of terrorism due diligence (AML/CFT, Article L.561-1 et seq. of the Monetary and Financial Code).

When anticorruption due-diligence is performed as a part of a comprehensive third-party due-diligence program, **corruption risk should be distinctly apprehended.**

Third pillar: Risk management

Risk prevention: Third-party due diligence (2/5)

Adapt third-party due diligence methods to risks

1. Identification of third parties
2. Categorization of third-parties in homogeneous groups according to risk profile based on the risk-map
3. Determination of due diligence methods adapted to the risk level of each category: simplified due diligence for “risk-free or low-risk" third parties; thorough due diligence for “high-risk” third parties
4. Within a category of third parties, due diligence is conducted on each third party separately: a third party can be reclassified after its individual assessment (incident, report, conviction, changes in behaviour)

An internal database dedicated to third-parties, compliant with applicable regulations, can usefully be set up.

Third pillar: Risk management

Risk prevention: Third-party due diligence (3/5)

Third-party due diligence in practice

WHO

- Operational staff responsible for due diligence
- Compliance department or professionals
- Top Management
- When due-diligence are outsourced, the company remains liable

HOW

- Company's internal lists
- Open-source information
- List of sanctioned natural and legal persons
- Business intelligence databases (commercialised by specialised service providers)
- Information from the third party (questionnaire, interview, audit, etc.)

WHAT

- Identity of the third party and leading shareholders
- Sensitivity to the industry corruption risk
- Experience, credentials and qualifications
- Negative reports, allegations or convictions
- Existence of an anticorruption programme
- Existence of relationships with public officials or politically exposed persons

Retention of information on third parties (confirmed by CNIL, the French Data Protection Authority): the entire third-party due diligence file and history of changes must be retained **for 5 years after the end of the business relationship** (or from the date of an occasional transaction), without prejudice to stricter legislation.

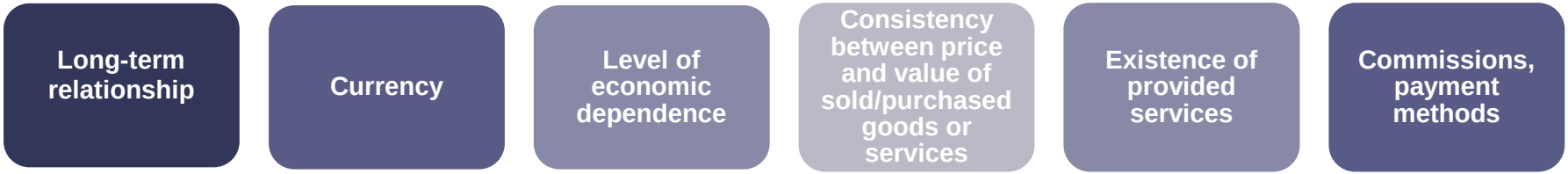
Third pillar: Risk management

Risk prevention: Third-party due diligence (4/5)

Assessment of the third party's risk level

- Risk factors regarding the nature of the third party

- Risk factors regarding the relationship with the third party



Third pillar: Risk management

Risk prevention: Third-party due diligence (5/5)

Conclusions from third-party due diligence

Based on the results of the due diligence

- **Approve the relationship** – with or without enhanced due diligence and mitigating provisions or controls
- **Postpone the decision** (e.g. pending further assessments)
- **Terminate or refrain** from entering into the relationship

The identification of risk factors does not rule out the relationship, but must lead the organisation to take appropriate steps to mitigate the risk.

Examples of mitigation strategies

- Communicate the company's **Code of conduct to third party**
- Raise **awareness of third party** to corruption risks through training for instance
- Require from the third party a **written commitment or include an anticorruption provision in a binding agreement**
- Encourage the third party to **check the integrity of its subcontractors**

Monitoring the contractual relationship

- Clear, detailed and formalized legal agreements
- **Careful monitoring of accounting schemes** and payments to and from risky third-parties

Renewing and updating third-party due diligence

- The **due diligence process is periodically performed** in accordance with the third party's category and related risk level
- **Re-performance of third-party due diligence at each significant change** (acquisition, etc.)

Third pillar: Risk management

Detection: Internal whistleblowing system (1/5)

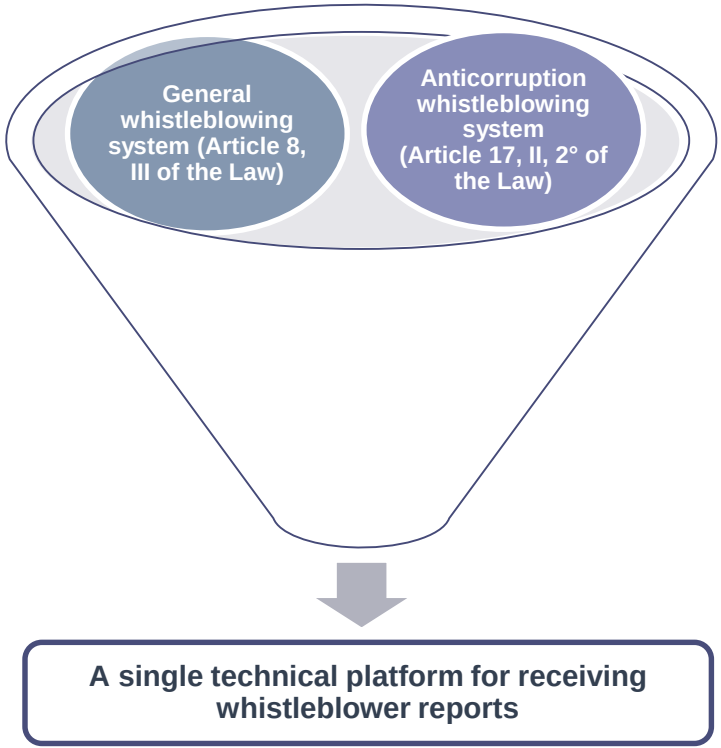
○ Definition

Procedure that companies implement to **enable their staff to inform** a dedicated contact person **about conducts or situations that violate the Code of conduct** so that they can be ended and the appropriate sanctions applied, where necessary.

○ Articulating different whistleblowing lines

Where multiple whistleblowing lines exist in the company as a result from different regulations, it is recommended to set up **a single technical platform for receiving whistleblower reports.**

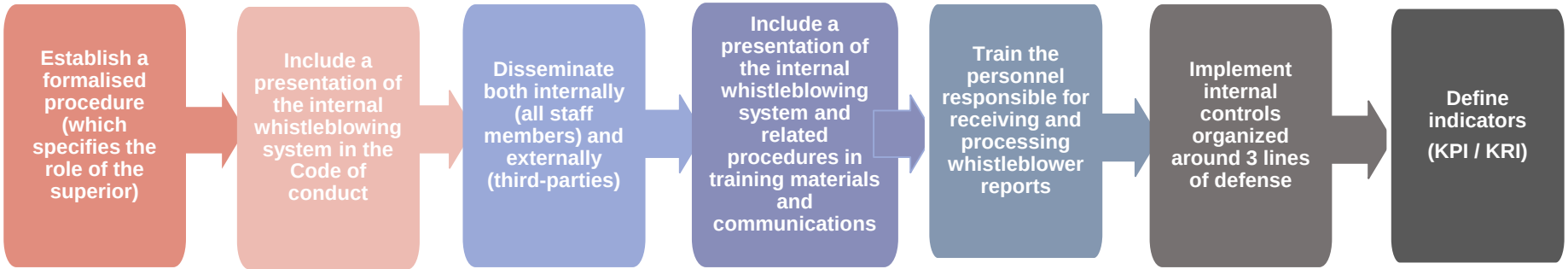
Subject to opening up the whistleblowing line to **company's staff but also to external collaborators and temporary workers** (*temporary staff, interns, service providers etc*.)



Third pillar: Risk management

Detection: Internal whistleblowing system (2/5)

Steps in the implementation of the internal whistleblowing system



Management of the system **may be outsourced**, provided the selected service provider has the **necessary qualifications** for processing whistleblower reports and meets **confidentiality** obligations.
Quality of service should be **regularly monitored** (through a SLA for instance)..

Third pillar: Risk management

Detection: Internal whistleblowing system (3/5)

Processing whistleblower reports

Procedure

- Reporting steps
- Report management / handling procedure
- Whistleblower protection regime
- Security provisions

Personnel

- Point of Contact (PoC), Report / Case handler
- The whistleblower: vigilance over protection of confidentiality
- Persons named in the reports

Security

- Access is restricted to preserve confidentiality
- Vigilance over the protection of evidence or documents
- Compliance with GDPR

Access and information

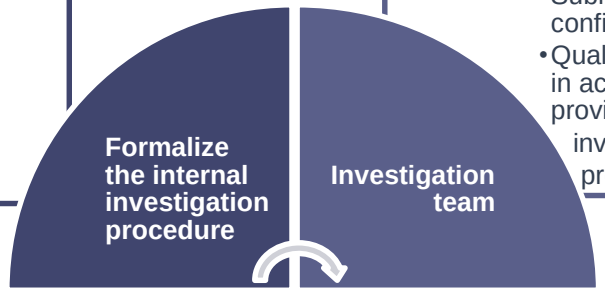
- Existing channels
- Conditions and circumstances as regard to information transfer
- Documents that may be used for an internal investigation
- Delivery notification
- Closing

Third pillar: Risk management

Detection: Internal whistleblowing system (4/5)

In the event of an internal investigation

- Criteria for initiating an investigation
- Procedures and methods for conducting an investigation



- Submitted to strict confidentiality
- Qualified and appointed in accordance with the provisions of the internal investigation procedure

- Disciplinary sanctions?
- Legal action?
- Update of the risk map

FURTHER ACTION

- Informed about most sensitive situations
- Decides what action to take

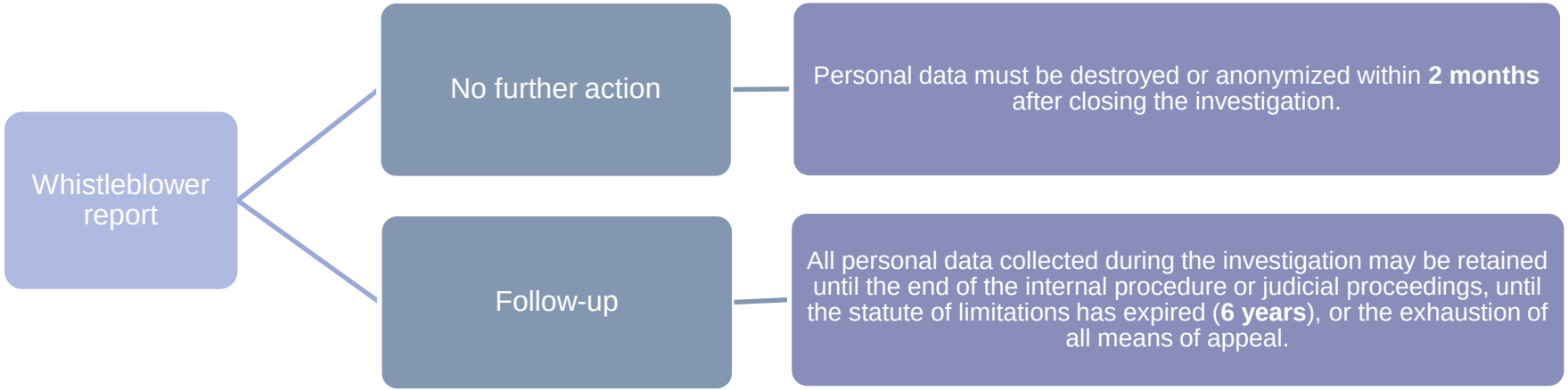
- Facts
- Methods
- Follow-up

If the investigation is outsourced, **the selected service provider must be subject to regular checks,** particularly with regard to compliance with confidentiality and data protection rules.

Third pillar: Risk management

Detection: Internal whistleblowing system (5/5)

Archiving whistleblower processing and their follow-up (confirmed by CNIL, the French Data Protection Authority):



Third pillar: Risk management

Risk detection: Internal control (1/4)

- **Three lines of defense**

1. Level 1 controls aims to ensure that operational and support processes are performed in compliance with corporate procedures.

- Performed by the operational or support staff or by their management

2. Level 2 internal control consists in testing randomly or at a predefined frequency the effectiveness of Level 1 controls to ensure that they are properly performed.

- Performed for instance by the compliance, quality, risk management or management control functions

3. Ensure that the internal control system complies with the applicable regulations and company's policies and is effectively implemented and maintained

- Performed by the audit function

- **Internal control and corruption prevention system**

The corruption risk map can be used to:

- Identify risk situations that are not or poorly covered by control measures;
- Evaluate the control systems in place to manage these risks.

Internal control:

- Covers situations identified in the corruption risk map when appropriate;
- Appropriately mitigates identified risks;
- Is regularly updated based on conclusions of internal control testing results.

The controls defined in this way are formalized under a procedure that specifies:

- Identified risks, related processes and situations,
- Control frequency and control procedures,
- Control owners,
- Reporting and anomaly management procedures.

Third pillar: Risk management

Risk detection: Internal control (2/4)

General accounting controls

- Provide reasonable assurance about the quality of accounting information.
- Ensures that the financials statements are prepared in accordance with generally accepted accounting practice and give fair and true view of the company's assets, liabilities, financial position and profit or loss.

Anticorruption accounting controls

- Designed consistently with regard to high-risk situations identified in **the corruption risk map**
- Aim in particular to detect unjustified or undocumented transactions.

Anticorruption accounting controls:

- Ultimately ensure compliance with the same principles as general-purpose accounting controls;
- Use the same methods as general-purpose accounting controls;
- But are based on the **CORRUPTION RISK MAP**.

Examples of high-risk situations that can be identified in a risk map:

- **Sponsorship, patronage**
- **Gifts, invitations**
- **High-stake transactions**
- **Transactions with high-risk third parties**
- **Off-balance sheet commitments (guarantees, collaterals, etc.)**

Some account items may involve a high level of risk, such as: reversing entries, discounts and rebates, sundry expenditures, cash floats, goodwill or suspense accounts and imprest accounts.

Third pillar: Risk management

Risk detection: Internal control (3/4)

Content of accounting controls

1st line of defense: accounting entries are properly justified and documented

- Persons responsible for booking and approving accounting entries
- Segregation of duties

2nd line of defense: controls the correct performance of the anticorruption accounting controls by the 1st line of defense

- Persons who are independent from those who performed the controls for the 1st line of defense
- All year long
- Sampling methods must be representative of the inherent risks in the transactions

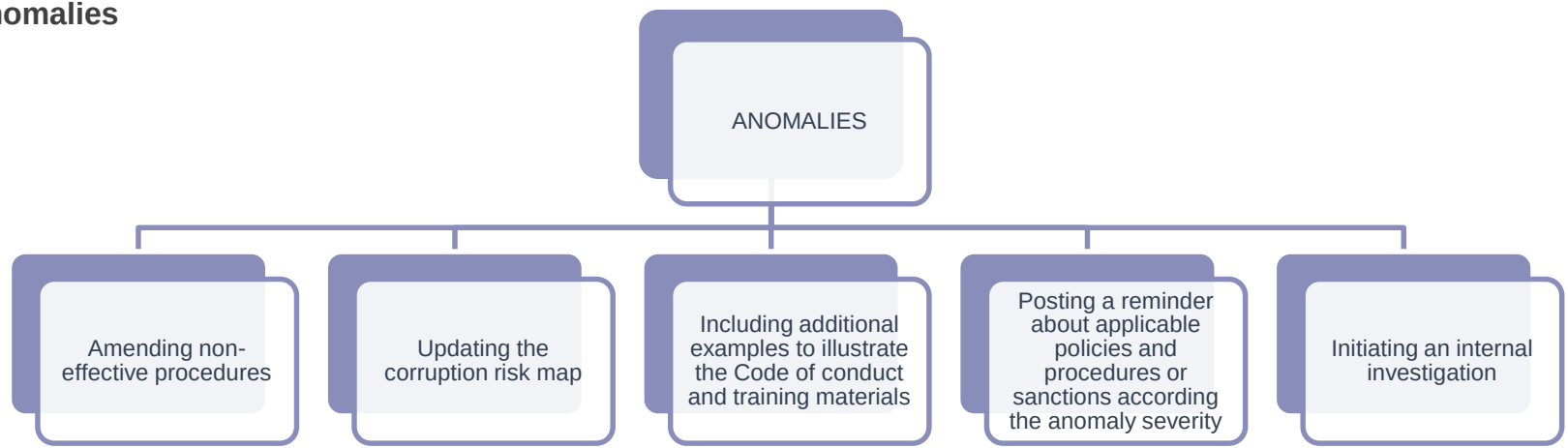
3rd line of defense: anticorruption accounting controls comply with corporate regulations, and are effectively implemented and up-to-date

- Governance and allocated resources are consistent with control objectives of the anticorruption accounting controls
- Methods that are selected to test the design and the effectiveness of the anticorruption accounting controls are consistent with the control objectives

Third pillar: Risk management

Risk detection: Internal control (4/4)

- **Anomalies**



- **Outsourcing**

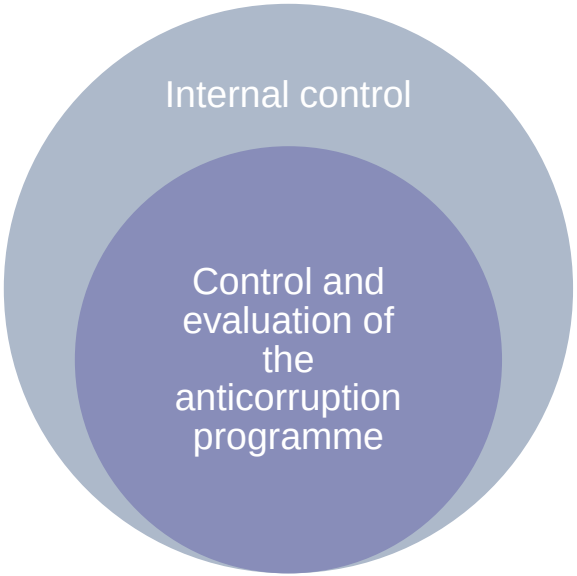
Accounting controls may be performed:
- **Internally**, by the accounting and finance departments or by specialized functions;
- **Externally**, by entities that the company mandates for this purpose.

Statutory auditors:
- **Contribute** to prevent and detect corruption;
- Legally required to **notify the prosecutor's office of any presumed criminal offense**, including corruption, uncovered when conducting an audit engagement.

Third pillar: Risk management

Control and evaluation of the anticorruption programme

Purpose and procedures



The internal control system aims to 4 objectives:

- Monitoring implementation of anticorruption programme elements and testing their effectiveness
- Identifying and understanding any anomaly in the application of the procedures
- Drafting recommendations or other appropriate corrective actions to improve the effectiveness of the anticorruption programme
- Detecting any corruption

Third pillar: Risk management

Corrective action

○ Management and follow-up of anomalies

Anomalies resulting from the unsatisfactory application of policies and procedures– and potentially reported by internal control campaigns and audits – are analysed to **identify their cause in order to take corrective action**.

○ Disciplinary system

The disciplinary system is composed of all disciplinary decisions that a company may take to sanction what it deems to be misconducts.

Misconduct results from **improper behaviors that do not comply with internal regulations**, for instance the provisions of the anticorruption Code of conduct.

The company is **not bound to wait for a criminal court decision** before imposing disciplinary sanctions, **if the misconduct is substantiated and serious enough to warrant sanctions**.

A sanction may only be imposed on a staff member **if it is provisioned in internal regulations and proportionate to the misconduct**.

Disciplinary sanctions may **be imposed based on the conclusions of a detailed internal investigation**.

The company may compile a report of disciplinary sanctions

- Strict confidentiality of its content;
- Compliance with personal data protection regulations.

Top Management may chose to communicate about imposed sanctions:

- In a way that guarantees total anonymity;
- To highlight its policy of zero tolerance for misconduct.

RÉPUBLIQUE FRANÇAISE

Liberté
Égalité
Fraternité

AFA
Agence Française Anticorruption

Thank you for your attention

For more information: https://www.agence-francaise-anticorruption.gouv.fr/files/files/joe_20210112_0010_0061.pdf

To contact the AFA: **afa@afa.gouv.fr**