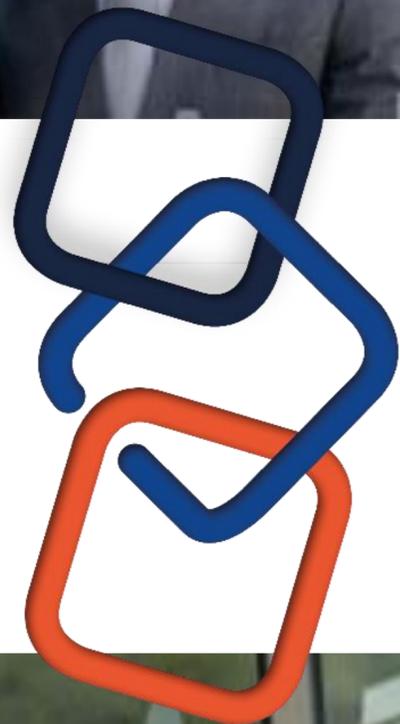




BELRiM

Belgian Risk Management Association



WHISTLEBLOWING

25/04/2023

In collaboration with PwC and ING



Exchange rules



Mute your mobile phone



Raise your hand if you want to interact during the Q&A



Give your name and your company when you interact



Presentation will be in English

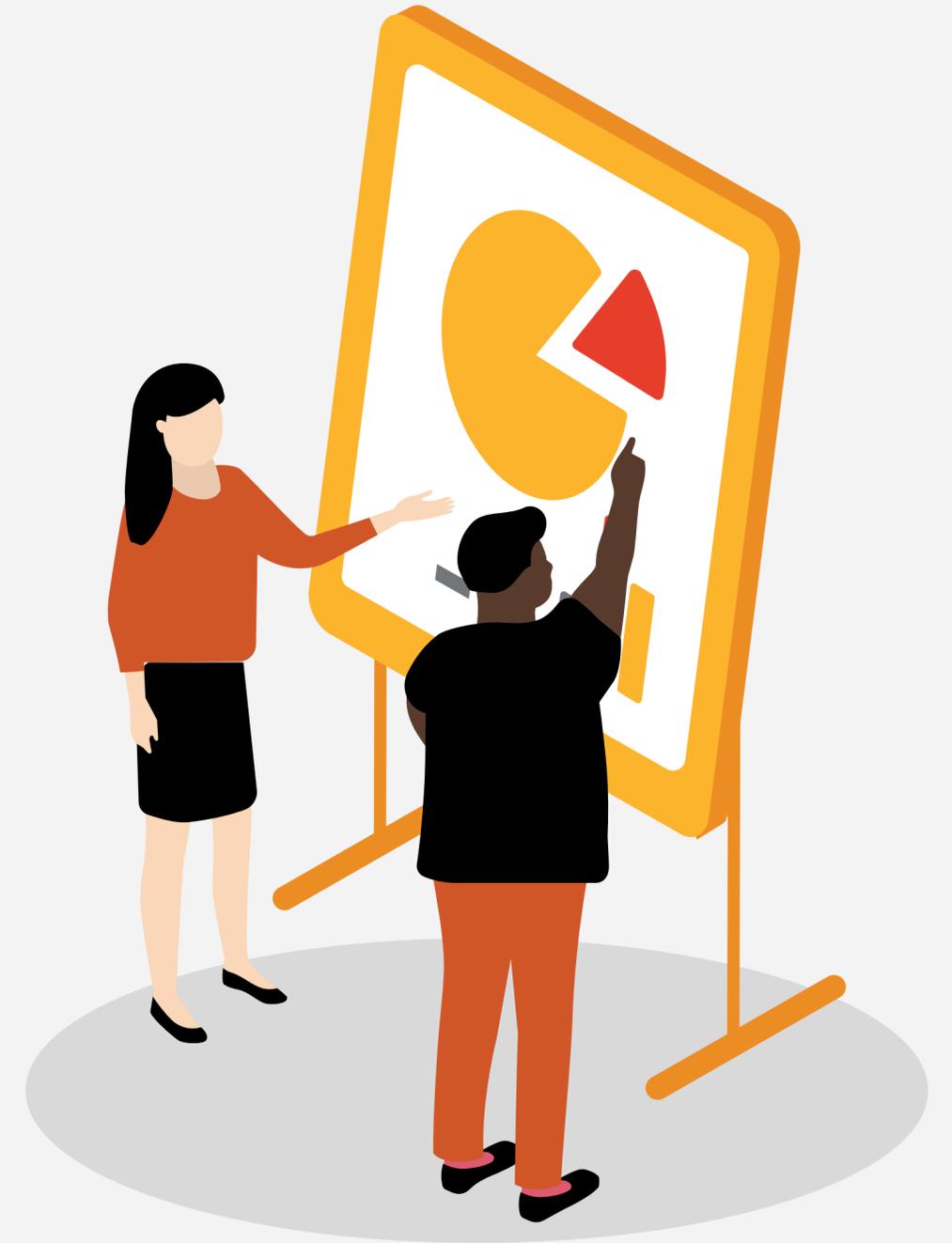


Pictures will be taken and might be used for communication

Agenda



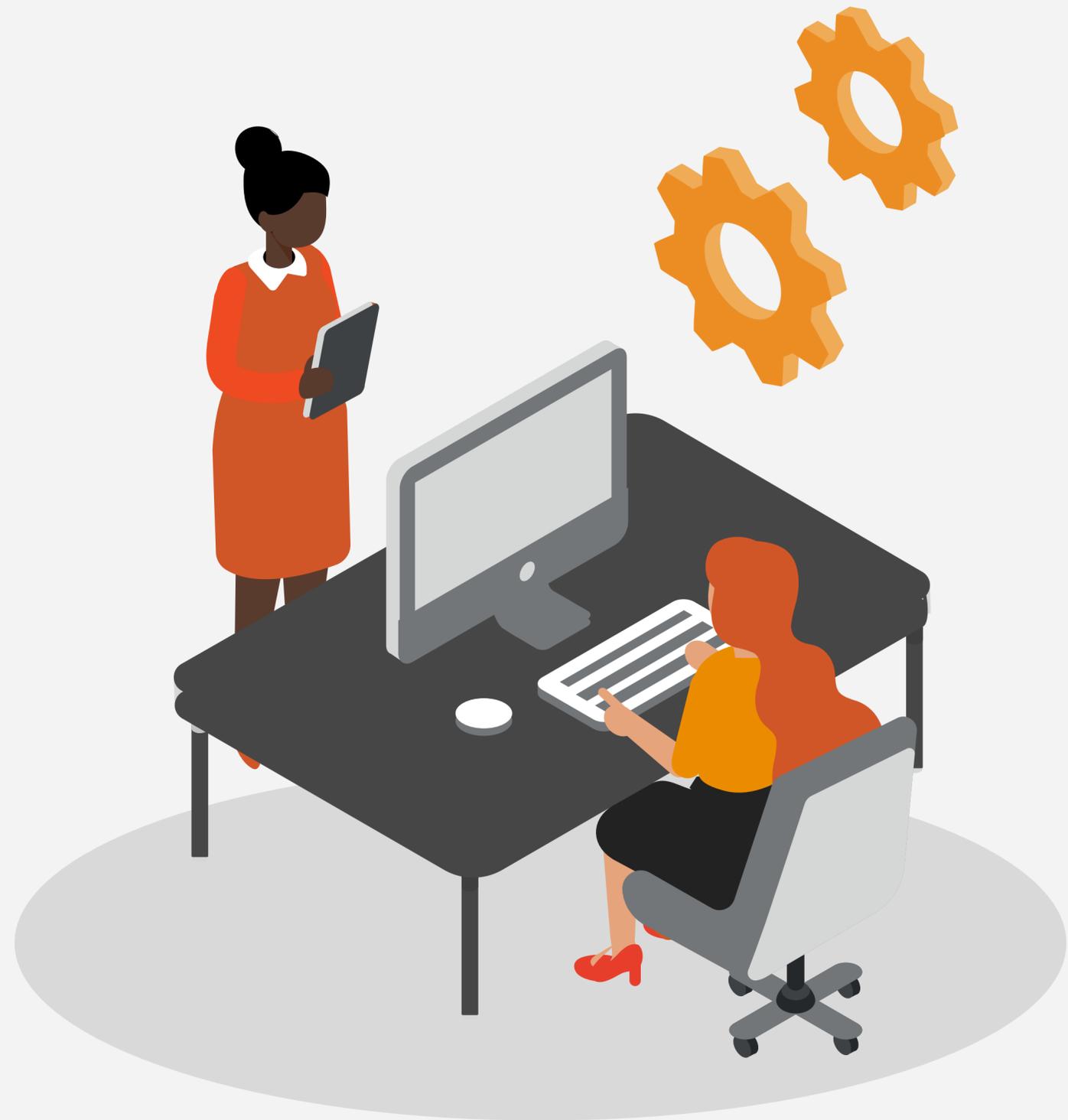
1	Legal Framework (30')
2	Whistleblowing: not just a regulatory matter (20')
3	Roles & Responsibilities for Whistleblowing (10')
4	ING testimony (30')
5	Q&A (30')



Legal

Framework

By Olivier Chapelle
PwC Legal



Legal framework

Status of the law in Belgium - Private sector



2019

Adoption of the Directive 2019/1937

The European Union adopts on **October 23, 2019** a directive containing rules on the protection of persons who report violations of EU law. This directive will now be known as the Whistleblowing directive.

2021

Deadline for the transposition of the directive

Belgium does not respect the transposition deadline of **December 17, 2021** and is facing sanctions from the European Union.

2022

Implementation of the Whistleblowing Directive (private sector)

On **November 28, 2022**, The Belgian parliament passed the Act transposing the Whistleblowing Directive. The Act is published on December 15, 2022 and will come into force on February 15, 2023.

2022

Entry into force of the Act (private sector)

The law came into force on **February 15, 2023**. For legal entities with 50 to 249 workers, the Belgian legislator grant a deferral to **December 17, 2023** except for the companies providing specific financial and economic services.

2022
-
2023

Implementation of the Whistleblowing Directive (public sector)

Depending on the region and the status of the implementation of the directive in the public sector, there are **several dates of entry into force**.

Legal framework

Private sector - a brief overview



What ?

The purpose of the Act is protecting individuals who report (potential) breaches of a number of specific areas which include:

- public procurements;
- financial services;
- product safety & compliance;
- protection of the environment;
- transport safety;
- radiation protection & nuclear safety;
- food and feed safety & animal welfare;
- public health & animal health;
- consumer protection;
- protection of privacy and data.

The Act reproduces the Directive's material scope verbatim, however, also expands on it by including **tax and social fraud** as well.

Who ?

A whistleblower is a person who reports (suspected) irregularities in an organisation or business.

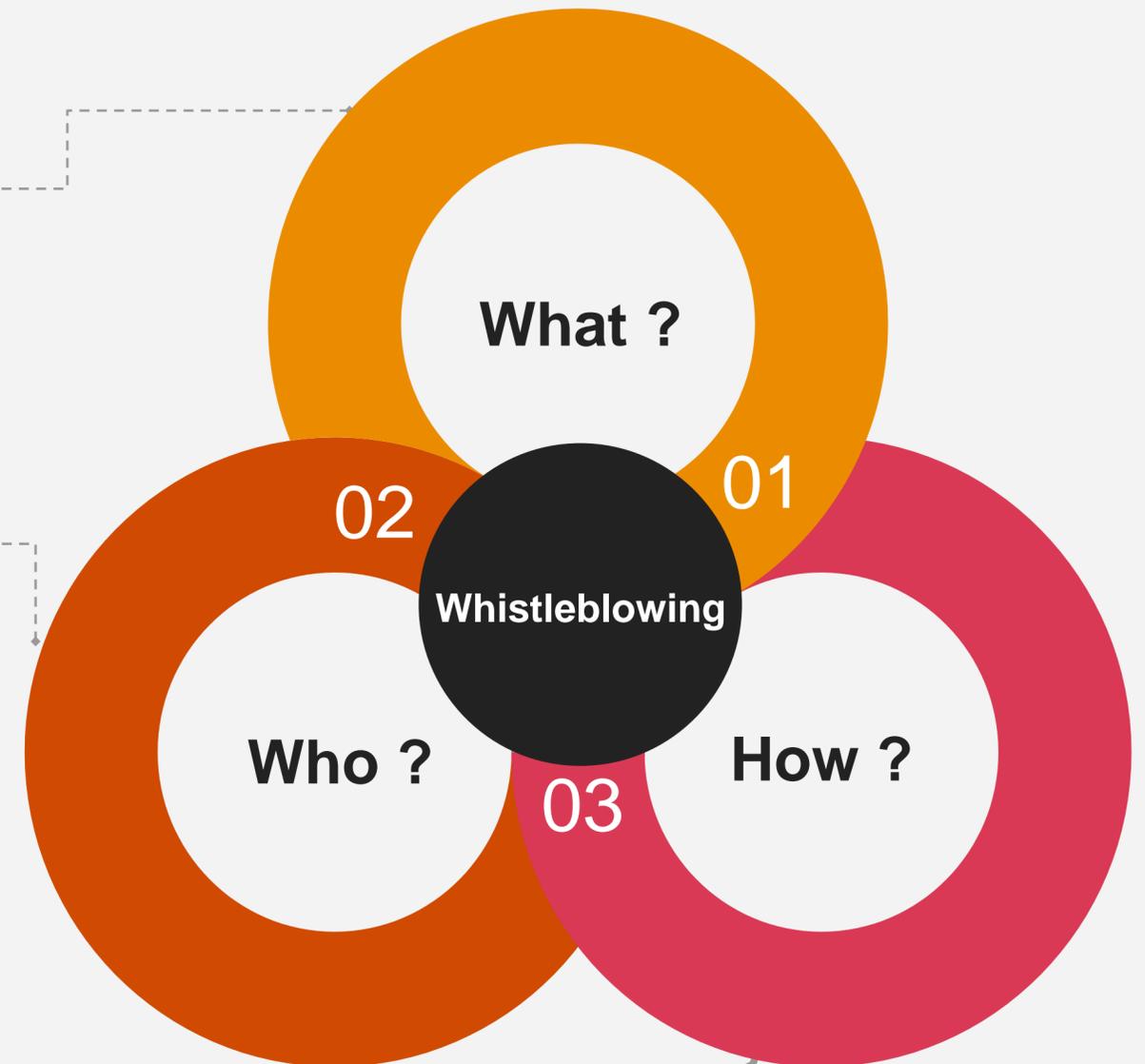
This person can be:

- an (ex-) employee;
- an intern;
- an external consultant;
- a shareholder or a board member;
- a supplier;
- ...

How ?

Reporting the violation can be done through three different channels (see hereafter). Whistleblowers can choose their reporting channel. There is no obligation to use the internal channel prior to the other two channels.

Even if the personal scope of the act seems broad, companies only need to provide at least an internal reporting channel for their workers.



Legal framework

Private sector - a brief overview



Internal channel

50 or more employees: The companies* have to set up an internal reporting system that has to be secure, impartial and confidential. Any report must be acknowledged within 7 days and answered within a maximum term of three months. However, companies providing specific financial and economic services have to establish an internal reporting channel as soon as they employ one employee.

This employee threshold concerns the average number of employees employed by the legal entity, calculated in accordance with the regulations that are applicable in the context of the social elections.

50 to 249 employees: Companies* can postpone the entry into force until **17 December 2023**.

250 employees or more: Companies* had to comply immediately upon the entry into force of the Belgian legislation on **15 february 2023**. Note that in those companies, reports can be filed anonymously. Companies with less than 250 employees are not obliged to process those anonymous reports.

**The definition of a company under the whistleblower Act is unclear and subject to debate. The company can be understood as a legal entity or a technical Business Unit.*



External channel

To introduce an external reporting channel, the Belgian transposition act designates the Federal Ombudsman as the coordinating body.

What is the role of the company then?

- ✓ Companies must inform workers of the procedures to follow for internal and external reporting;
- ✓ Despite external reporting, workers will still fall within the scope of the law and will therefore be protected.



Public disclosure

Where a prior internal or external whistleblowing doesn't result in appropriate action (1) or if there are serious reasons to believe that there's an immediate threat to the public interest, or if there's a risk of retaliation or destruction of evidence (2), a reporting can also be done via public disclosure.

Legal framework

Obligations for private companies



Setting up an internal reporting channel and procedures to ensure follow up

- Establishment of secured channel **after consultation with the social partners**.
- Implementation of an internal policy for at least the reporting of the workers of the company. The policy must always comply with the most stringent local rules, if any. A global standard policy with a country-specific annex that provides for necessary deviations can therefore be provided.
- Designation of a (internal or external) report manager who will follow up on the file with diligence:
 - **Acknowledgment within 7 days;**
 - **Follow-up of the complaint within 3 months.**

Information

- Companies must inform workers of the procedures to follow for internal **and** external reporting.
- The procedures must be clear and accessible to the workers. For example:
 - The entity can give a seminar to its workers; and
 - The entity can display the procedures within the premises of the company.

Confidentiality, anonymity and protection

- The channels are designed to ensure **confidentiality**.
- Personnel handling whistleblowing data must do so in strict confidentiality.
- The identity of the whistleblower is confidential as well as the information he delivered.
- For companies counting 250 employees or more, **anonymous reports** can also be filed and must be treated.
- Whistleblowers are **protected against retaliation** or threat of retaliation.

Legal framework

Protection



Whistleblowers are protected against retaliation or threat of retaliation if the whistleblower:

- has reasonable grounds to believe that the matters reported by them are true and fall under the material scope; **and**
- reports the violation via one of the three reporting channels: internal channel, external channel or public disclosure.

Retaliation can take all kind of forms such as:

- Suspension
- Dismissal
- Demotion
- Withholding of promotion
- Changing the terms of the employment
- Intimidation
- Blacklisting



A whistleblower who suffers retaliation is entitled to:

- an indemnity that ranges between 18 and 26 weeks salary; or
- if the whistleblower is no employee, equals the actual damages.

In case of retaliation after reporting a breach related to financial services, products and markets, or the prevention of money laundering and financing of terrorism, the whistleblower can choose between:

- an indemnity that's equal to 6 months salary (of course only possible for employees); or
- one that equals the actual damages.



Legal framework

Penalties for non-compliance



Potential personal liability for the members of the board of directors.



Type of offence	Sanctions
<p>Non-compliance with the obligation to set up an internal reporting channel will be sanctionable with a level four Social Penal Code sanction for the employer, its agent or its representative / proxy holder.</p>	<p>either imprisonment of six months up to three years (converted for legal entities into a fine of EUR 24.000 up to EUR 576.000*); and/or a criminal fine of EUR 4.800 to EUR 48.000 or an administrative fine of EUR 2.400 to EUR 24.000.</p>
<p>A private sector legal entity (employer, its agent, its representative / proxy holder), the members of its personnel, as well as each natural person who:</p> <ul style="list-style-type: none"> • impedes or tries to impede a reporting; • retaliates against a whistleblower; • initiates unnecessary and vexatious proceedings against a whistleblower or; • violates the obligation to keep a whistleblower's identity confidential. 	<p>will also be punishable by imprisonment of six months up to three years (converted for legal entities into a fine of EUR 24.000 up to EUR 576.000*); and/or a criminal fine of EUR 4.800 to EUR 48.000.</p>

*For companies, prison sentences must be converted into monetary penalties:

- The minimum sentence of imprisonment is converted in a minimum fine of : $EUR\ 4.000 \times$ the number of months corresponding to the minimum of the imprisonment, but not less than the minimum of the fine provided for the law;
- The maximum sentence of imprisonment is converted into a maximum fine of: $EUR\ 16.000 \times$ the number of months corresponding to the maximum of the imprisonment, but not less than twice the maximum fine provided for the law.

Legal framework

Relation with prior legislation



→ The whistleblower act does not affect other existing procedures in Belgian labour law. However, what about the cumulation of indemnities?

CBA 109 regarding the motivation of dismissal	The compensation cannot be cumulated with any other compensation due from the employer on termination of the employment contract , with the exception of : <ul style="list-style-type: none">- compensation in case of notice,- non-competition compensation,- eviction compensation or,- supplementary compensation that is paid in addition to social security benefits.
Act on well-being at work (procedures in case of harassment)	Accumulation is not explicitly forbidden
Indemnities in case of dismissal	Accumulation is not explicitly forbidden
Other indemnities	Until proven otherwise, all existing compensation coexist except for those granted on the basis of CLA 109

Legal framework

Federal public sector



→ The Act of 8 December 2022 “concerning the reporting channels and the protection of persons reporting integrity violations in the federal public authorities and in the integrated police” has been published in the Belgian Official Gazette on 23 December 2022 and will enter into force 10 days after its publication, i.e. on 2 January 2023.

In contrast to the Act applicable in the private sector, no period of two months between publication and entry into force was decided.

The law applies to "federal public sector bodies". This includes:

- **federal administrative authorities** (e.g. SPF, SPP and autonomous public enterprises),
- **strategic bodies** (see Royal Decree of 19 July 2001), and
- **all other bodies or services that are dependent on the federal authorities and do not belong to the private sector**, such as the Federal Ombudsmen and the Data Protection Authority.

Legal framework

Regional public sector



Dutch Region	Walloon Region	Brussels Capital Region
<p>Decree of 18 November 2022 amending the Provincial Decree of 9 December 2005, the Decree of 22 December 2017 on local government and the Governance Decree of 7 December 2018, with regard to whistleblowers.</p>	<p>Decree of the Walloon Government of 13 October 2022 concerning various provisions related to the reporting of information on suspected irregularities within a service of the Walloon Government or a public interest organization to which the decree of January 22, 1998, relating to the status of personnel of certain public interest organizations under the jurisdiction of the Walloon Region applies - <i>Main transposition of the Directive.</i></p> <p>Decree of 21 December 2022 on the waiving of professional secrecy in the event of the reporting of information on a suspected irregularity within a Walloon Government department or a public interest body to which the decree of 22 January 1998 on the status of the personnel of certain public interest bodies under the authority of the Walloon Region is applicable - <i>Partial transposition of the Directive.</i></p>	<p>Draft joint decree and ordinance of 23 May 2022 of the Brussels-Capital Region, the Joint Community Commission and the French Community Commission amending the joint decree and ordinance of 26 April and 16 May 2019 on the Brussels Mediator</p> <p>Rules of procedure of the Brussels mediator (joint decree and order of 16 May 2019 relating to the Brussels mediator)</p>
<p>This decree offers protection to all whistleblowers working in the Flemish public services, whether they are internal or external staff, as well as freelancers, volunteers or interns.</p>	<p>The main transposition of the directive provides for protection against reprisals for "whistleblowers", i.e. staff of the Walloon regional civil service who report suspected irregularities if they are detrimental to or threaten the general interest and if they constitute a violation of the applicable rules or involve a significant risk for citizens or the environment.</p> <p>The partial transposition of the directive provides for specific rules regarding the breaching of professional secrecy.</p>	<p>This draft decree aims to offer protection to all whistleblowers working in the Brussels public services, whether they are internal or external staff, as well as freelancers, volunteers or interns.</p>

Legal framework

Local public sector

Session of the Housing and Local Authorities Committee of the Walloon Parliament of 21 March 2023

→ Parliamentary question asked to Minister Collignon* on the implementation of a system protecting whistleblowers within local authorities

Two draft decrees were adopted and transmitted to Parliament on Wednesday 15 March 2023;

- The draft decrees have yet to be submitted for parliamentary debate;
- The texts have not yet been published.

**Minister for Local Authorities*



Legal framework

Federal public sector vs. Private sector



Points of attention

Threshold	Unlike the private sector, all public sector entities are required to set up an internal reporting channel, regardless of the number of employees (except if the legislator provides for an exemption for small local authorities or other public bodies with less than 50 employees).
Anonymous reporting	Anonymous reporting is always possible within the public sector unlike the private sector, where this type of reporting must be provided by companies with more than 250 employees.
No cascade procedure	The three modes of reporting (internal reporting, external reporting and public disclosure) are on an equal footing.
Internal reporting	Internal reporting is in principle addressed within the public sector body itself.
External reporting channel	The external reporting channel is established with the federal ombudsman.

Global regulatory requirements



EU/Belgian legislation follows global trend

Canada

Public Servants Disclosure Protection Act(s) (protection of public sector employees, does not apply to private sector)
Competition law
Occupational health and safety laws

United-Kingdom

Public Interest Disclosure Act
UK Anti-Bribery Act

“An employer with at least 50 workers will must have a documented internal procedure to enable employees to raise concerns about wrongdoing and to protect them from retaliation.”

The Netherlands

The House of Whistleblowers Act

“Sarbanes-Oxley also prohibits retaliation against employee whistleblowers under the obstruction of justice statute.”

“Les procédures [...] pour recueillir les signalements [...] garantissent une stricte confidentialité de l'identité des auteurs du signalement, des personnes visées par celui-ci et des informations recueillies par l'ensemble des destinataires du signalement. [...] Les éléments de nature à identifier la personne mise en cause par un signalement ne peuvent être divulgués, sauf à l'autorité judiciaire.”

United States

Foreign Corrupt Practices Act and Securities Exchange Act (whistleblower compensation statutes)
Sarbanes-Oxley Act 2002

Brazil

Brazilian Anti-Corruption Law and Decree 11,129/2022

Australia

Corporations Act (from 1 July 2019, the whistleblower protections in the Corporations Act have been expanded)
Public Interest Disclosures Act in New South Wales



Whistleblowing, not just a regulatory matter

By Ben Colson
PwC Risk Consulting



Effective way to detect fraud and corruption



Whistleblowing allows you to identify fraud and corruption issues early

XX%

XX% of forensic investigations conducted by PwC in Belgium are a direct consequence of a whistleblower report.

XX%

XX% of fraud is detected by a tip.
(Report to the Nations” 2020: Global Study on Occupational Fraud and Abuse, ACFE)

XX%

Fraud losses were XX% smaller at companies with a whistleblowing platform
(Report to the Nations” 2020: Global Study on Occupational Fraud and Abuse, ACFE)

Effective way to detect fraud and corruption



Whistleblowing allows you to identify fraud and corruption issues early

75%

75% of forensic investigations conducted by PwC in Belgium are a direct consequence of a whistleblower report.

43%

43% of fraud is detected by a tip.

(Report to the Nations” 2020: Global Study on Occupational Fraud and Abuse, ACFE)

49%

Fraud losses were 49% smaller at companies with a whistleblowing platform

(Report to the Nations” 2020: Global Study on Occupational Fraud and Abuse, ACFE)

Effective way to detect fraud and corruption



Learnings from the U.S.' SEC's whistleblower programme where whistleblowers are rewarded for specific, credible and timely tips that are accompanied by corroborating documentary evidence

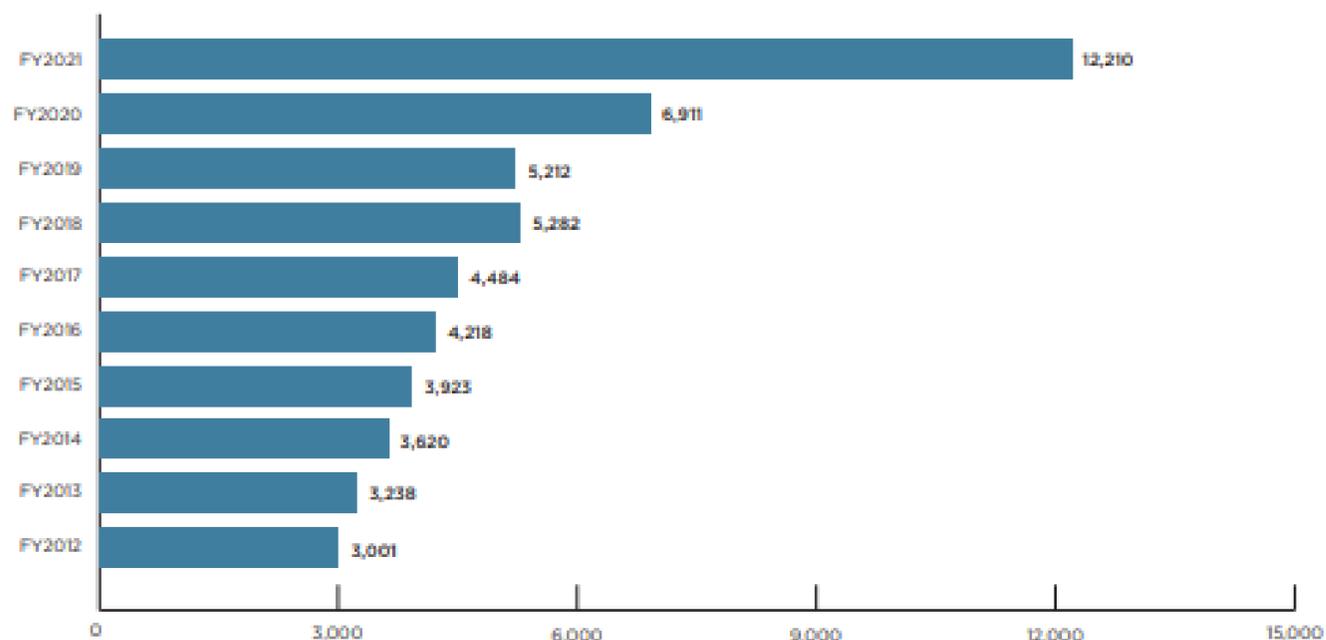
In FY 2021, the SEC received over **12,200 whistleblower tips**.

A significant increase compared to FY 2020, see table below.

In FY 2021, the **most common complaint** categories were:

- Manipulation (25%);
- Corporate disclosures and financials (16%);
- Offering fraud (16%).

In FY 2021, the Commission awarded approximately \$564 million to 108 individuals.



Since the inception of the programme:

- the SEC awarded more than **\$1.1 billion to 214 individuals** for information that led to the success of enforcement actions.
- **\$5 billion in total monetary sanctions, including more than \$3.1 billion in disgorgement of ill-gotten gains and interest, of which more than \$1.3 billion is scheduled to be returned to harmed investors.**

Essential part of any effective compliance programme



Whistleblowing contributes to identifying compliance and ethics issues

A compliance lens

- Whistleblowing is essential to **identify** and **remedy non-compliance issues early and internally**. E.g. in relation to competition law violations or safety issues. Allows the company to address these issues prior to them resulting in public disclosures and reputational damage.
- Component of the broader **Incident Management Framework**, that defines how the organisation identifies, assesses, tracks, manages and reports incidents. Identifying incidents timely is critical for managing and recovering from the incident.

An ethical lens

- A significant share of reports through whistleblower channels relate to **unethical conduct** such as bullying, harassment (physically, verbally, sexually, gender) and diversity.
- Whistleblowing can **make** management and the Board **aware of a suboptimal company culture** that can have financial, reputational and operational impacts.
- Accessible whistleblowing channels allow management to **foster a speaking-up culture** and **an environment of trust** within the company.



Essential part of the risk management programme

Whistleblowing contributes to identifying and responding to risks



COSO - Enterprise Risk Management: Integrating with strategy and performance (June 2017 - Volume I, p.21-22)

Per the **COSO** framework, you must **identify internal and external events that affect the achievement of the organisation's objectives.**

Additionally, you must **assess and respond to the risk** with appropriate actions that align with risk tolerance and risk appetite of the organisation.



Whistleblowing is critical to identifying red flags and issues across all risks domains and that allows you to manage risk through effective response.

Stakeholder management

Stakeholders expect demonstrable actions

- **Customers, shareholders** and the **general public** are increasingly emphasizing **ethical business practices**; whether it is in the context of anti-bribery and corruption, fraud, ethics in the supply chain, as well as for **environmental, social and governance** reasons.
- They expect companies to **act responsibly** and to take these topics at heart.
- Being able to **demonstrate an effective compliance and ethics programme** is therefore crucial.
- Whistleblowing mechanisms, that are **open to the public and your suppliers, customers and other stakeholders** are essential to **demonstrate** you 'walk the talk'.



Roles &

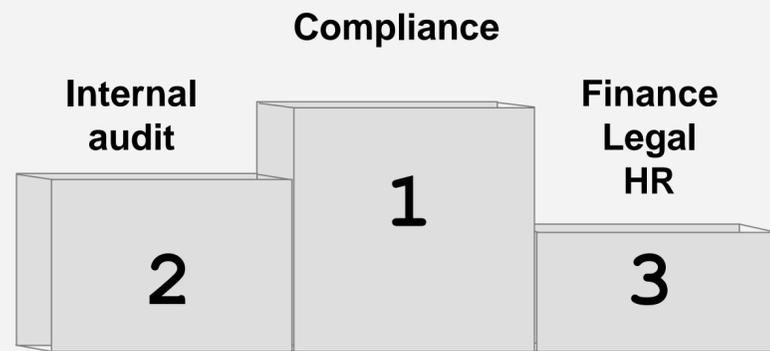
Responsibilities

By Ben Colson
PwC Risk Consulting



Roles and responsibilities

The **ownership** of the whistleblowing programme should be in the hands of either:



Compliance experts are independent (2nd line) and familiar with establishing governance structures and compliance frameworks.



Legal counsel provides support in:

- Interpretation of the legislation prior to drafting policies.
- Performing a quality check of the drafted policies to ensure compliance with applicable legislation.
- Assessing the repercussions of initiating an investigation and assuring the legality of the procedures and the admissibility of acquired information.

Outsourcing parts of the management and response to whistleblower reports to external providers may be appropriate



Triage support

Provide support in the initial stages of the report:

- To assess the gravity and impact of the report.
- Triage in order to minimise time spent on the initial assessment of cases.



Forensic professionals are an added value in investigations for the following reasons:

- Sound investigative methodology through experience.
- Independence as an outside investigator and absence of bias.
- Availability of resources.
- Technical skills and availability of appropriate technology.



Responsibilities of the owner



Elaborating a **framework** with:

- Clarity on roles and responsibilities.
- Understanding of legal and regulatory requirements: (inter)national
- Effective policies and standard operating procedures.
- Training & communication to create awareness.



Ensure **operational efficiency & independence** throughout the process via

- Clear governance structures.
- Standard flows.



Ensure **qualitative & complete investigation**

- Involve (external/legal) experts.
- Forensic technology to analyse (un)structured data sets.



Ensure **internal follow-up, reassurance** of the **whistleblower** and **credibility** of the programme through communication

- Clear action plan to avoid future repetition.
- Proactive and regular communication with the WB.
- Firm wide communication about reports and follow-up actions.

Design pitfalls



DO's



Adequate framework

How?

- Tailor policies to the size of the organisation
- Determine local/international scope



Operational efficiency & independent investigation

How?

- Clear governance structures
- Standard flows



Qualitative & complete investigation

How?

- Involve (external/legal) experts
- Forensic technology to analyse (un)structured data sets



Follow-up internally

How?

- Clear action plan
- Proactive and regular communication with the WB

DON'Ts



Inform new joiners only

Instead:

- Include in onboarding (involve HR)
- All staff need to be aware & trained
- Regular repetition



Start investigating without consulting a legal counsel

Instead:

- Consult to ensure compliance with data protection & local labour laws



Wait to set up a framework contract

Instead:

- Act swiftly, set-up framework contracts early



Rely only on WB to detect anomalies

Instead:

- Set-up a robust internal control environment
- Audit & monitor continuously

Implementation pitfalls



DO's



Stakeholder involvement

How?

- Get their input soon in the process



Functional requirement definition

How?

- Understand your own needs first
- Differentiate between *need-to-have's* and *nice-to-have's*



Company culture development

How?

- Promote reporting of unethical behaviour
- Change the culture through repetitive communication

DON'Ts



Rely on the number of reports today to determine investment

Instead:

- See the potential of a robust compliance programme



Design during configuration of the tool

Instead:

- Avoid additional costs
- Think ahead of your needs combined with stakeholder input



Refrain from modifications after initial configuration

Instead:

- Reflect on any improvement needs and put in place an ongoing improvement process.

Final message



What are three main reasons given by people for not reporting wrongdoing (per Transparency International):

1. Fear of the consequences (legal, financial, reputational)
2. The belief that nothing will be done, that it will not make any difference
3. Uncertainty about how, where and whom to report?

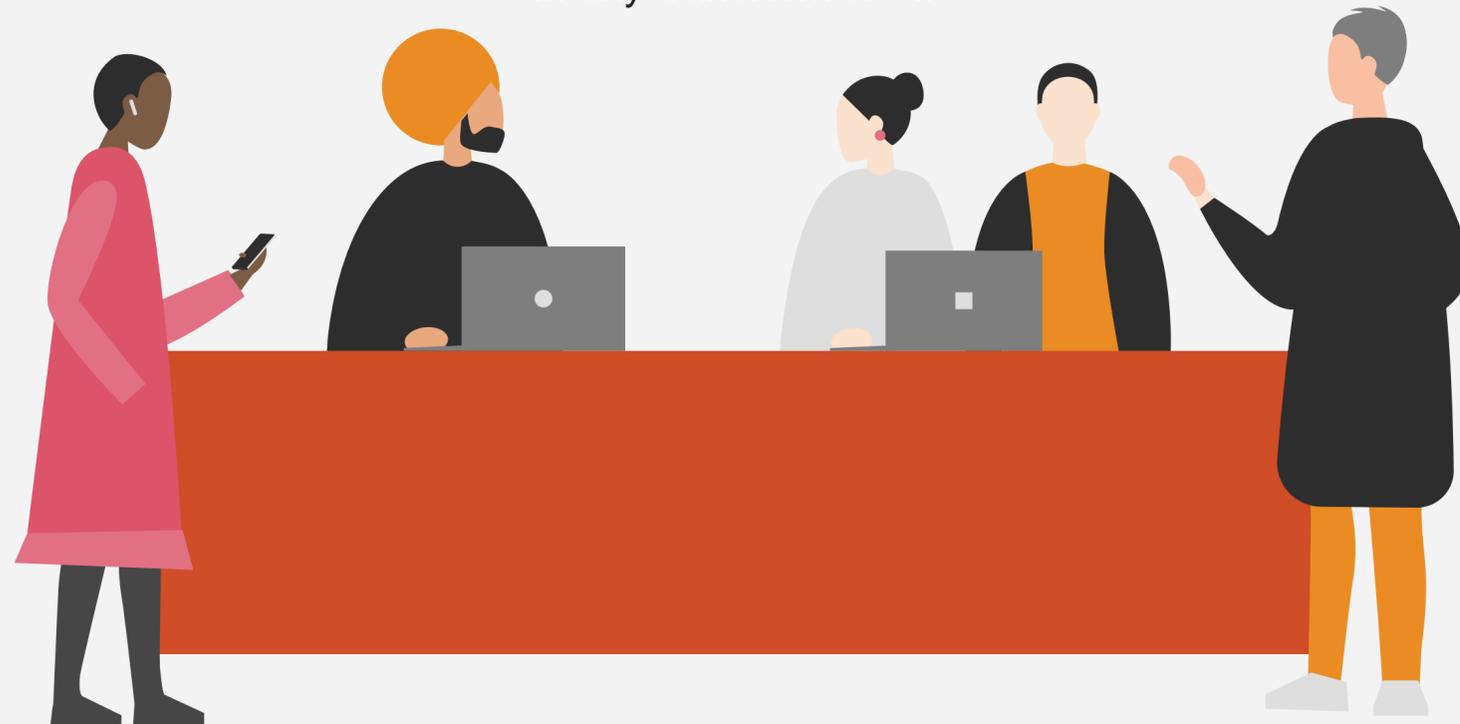


Companies should keep these reasons in mind when developing the whistleblowing policies and procedures for their organisation.

Addressing these 3 concerns should be at the heart of the implementation.

Communication & training are key

1. Draft policies and communicate about it to **reassure your people** about independence & confidentiality.
2. **Communicate about your efforts** both in terms of cases handled as well as actions taken from these investigations
3. **Communicate on regular intervals with the whistleblower** about the progress & status of the case assessment.
4. Provide training & repeat regularly where to report. **Repetition is key** in any transformation.



PwC Legal
A multidisciplinary law firm



Technological

Support

By Ben Colson
PwC Risk Consulting



Technological support



Facilitation of reporting and case management

Complement existing channels with a digital solution, ensuring anonymity for the whistleblower and assisting you in incident management.



Reporting channel **available 24h/day**, 365 days/year, also on the **mobile devices** of your employees (mobile friendly)



Security as top priority



Communicate with (anonymous) whistleblower



Logs which allow **audit & monitoring**



Up-to-date compliance with national legislation



Available to **internal and external stakeholders**



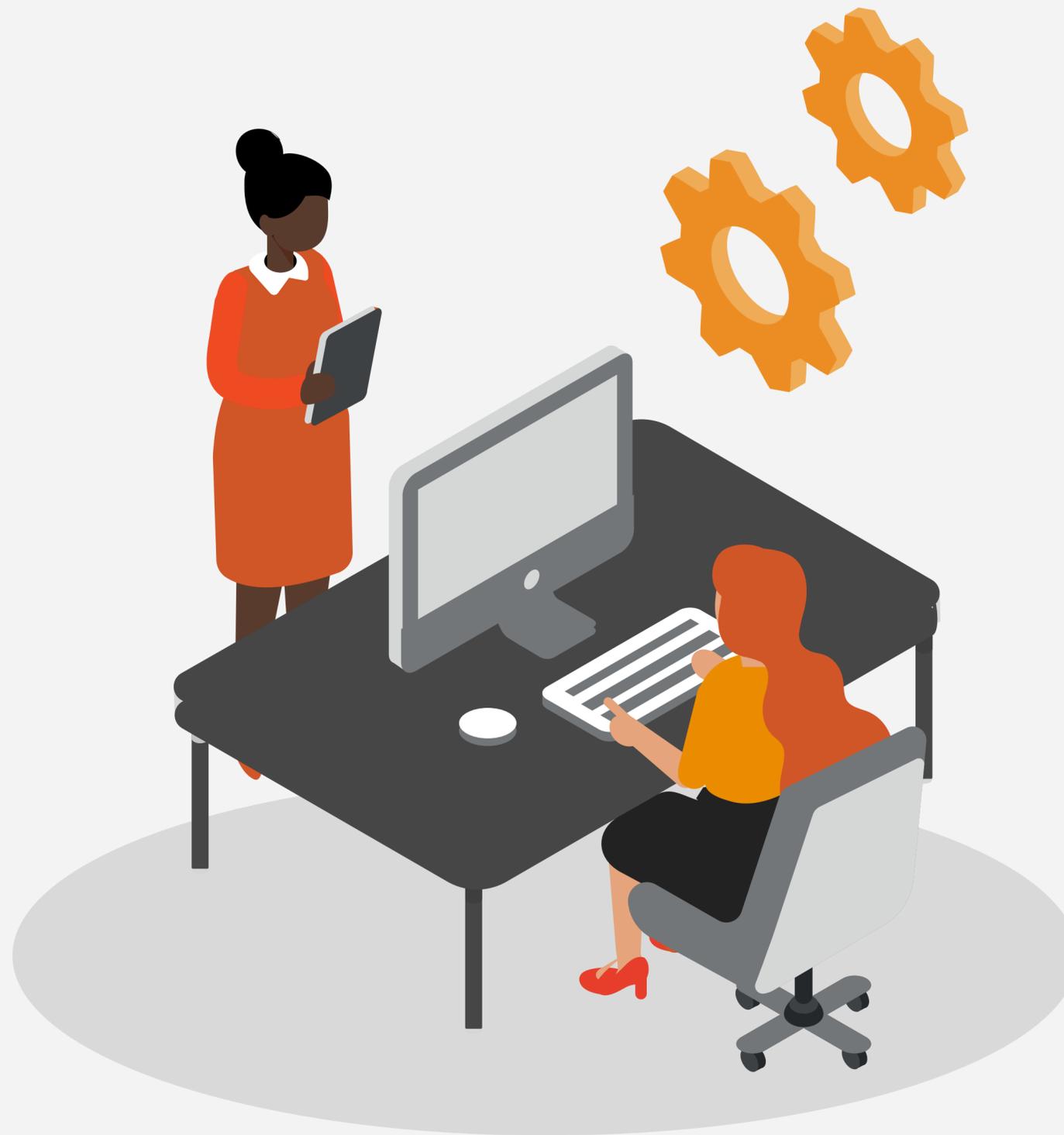
Don't underestimate the selection of a tool, as this can be challenging:

- Determine the core requirements for a whistleblower tool to facilitate the decision-making process for an enabling technology.
- Short listing of software providers
- Objectively compare the offers taking technical, functional and financial requirements into consideration.

ING

Implementation

By Sabine Desantoine
ING Belgium



(Pre-)Existing legal context for the financial sector



- Law of July 31st 2017 providing for the notification of actual or suspected violations of financial laws/regulations to the FSMA
- Law of 18th September 2017 on Anti-Money Laundering (AML) providing for a similar reporting regime of AML breaches to the CTIF
- Law of 22nd February 1998 on NBB (Nationale Bank-Banque Nationale) providing for a prohibition of retaliation to the whistleblowers who report infringement of the laws governing the legal status and supervision of financial institutions to the NBB



Already present: Whistleblowing Reporting Officers, WB policy, reporting channels, investigation means, ...



GLOBAL

- Adaptation of the Group Whistleblower policy to the EU Directive

LOCAL - Belgium

- Enhancement of the internal communication – Speak up campaign
- New and additional Whistleblowing Reporting Officers
(6 entities - specific training received)
- Adapted internal reporting channel to reinforce the possibility of anonymous calls

Awareness campaigns



In the spotlight



Speak up channels

- ING in Belgium
- Available in: English, Français, Nederlands

When you see or experience something that isn't or doesn't feel right, please speak-up and contact our trusted counsellors, external prevention advisors psychosocial aspects or whistleblowing reporting officer. They are there to help you.

Once the new BE law has been published



Working group established

Who are your main stakeholders?

- Compliance – Whistleblowing Reporting Officers
- Legal
- Human Resources – Legal Human Resources
- Communication
- Prevention Advisors / Persons of Trust
- Inspection
- Operational Risk Management

Once the new BE law has been published



What are the steps undertaken?

- Gap analysis (EU Directive – BE transposing law – other existing laws)
- Risk assessment
- Alignment with Prevention Advisors & Persons of Trust
- Adaptation of the Register of Processed Activities (Ropa)
- Adaptation of the Group policy – BE addendum
- Guidance for WBRO
- Presentation to the Risk Committee and to the Unions (Committee Social Law)
- Update intranet and internet pages
- Internal communication to all staff



Pitfalls to avoid...

- Don't prepare the implementation in your corner
- Select and appoint the right and adequate person(s) as WBRO
- WBRO: prepare script for reporting/interview moments
- Prepare clear and easy to understand information on the Speak up/WB channels (which ones, process, expectations, confidentiality, protection, ..)
- Look for local languages usage
- A whistleblowing report is not a complaint on your company services/products – Make the distinction!

Q&A

Moderated by the speakers
PwC and ING



Closing

note

By Adriana Cavaliere
Belrim - Skeyes





Don't miss out on our next events

30/05/2023 BELRIM Stamcafé – Risk Reporting

22/06/2023 BELRIM General Assembly + HDI Exchange on C.A.R.

29/06/2023 BELRIM Stamcafé – Artificial Intelligence

FERMA European Risk Management Awards: **Deadline 19/05/2023**

Thank

you!

