A white text on a black background

Description automatically generatedInternal whistleblowing systems

**Self-assessment framework**

Transparency International is a global movement with one vision: a world in which government, business, civil society and the daily lives of people are free of corruption. With more than 100 chapters worldwide and an international secretariat in Berlin, we are leading the fight against corruption to turn this vision into reality.

**www.transparency.org**

Author: Marie Terracol

ISBN: 978-3-96076-259-1

2024 Transparency International. Except where otherwise noted, this work is licensed under CC BY-ND 4.0 DE. Quotation permitted. Please contact Transparency International – [copyright@transparency.org](mailto:copyright@transparency.org) – regarding derivatives requests.

A close up of a logo

Description automatically generated



This publication was produced as part of the “SAFE4Whistleblowers” project, which was funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor the granting authority can be held responsible for them.

Internal whistleblowing systems

Self-assessment framework for public and private organisations

# Table of contents

[Acknowlegements 5](#_Toc180672143)

[Glossary 6](#_Toc180672144)

[Acronyms 7](#_Toc180672145)

[Introduction 8](#_Toc180672146)

[Who should implement internal whistleblowing systems? 9](#_Toc180672147)

[Conducting the self-assessment 12](#_Toc180672148)

[Roles and responsibilities in conducting the assessment 13](#_Toc180672149)

[Assessment framework: dimensions and questions 13](#_Toc180672150)

[Instructions for Completing the framework 14](#_Toc180672151)

[Analysing the answers and defining follow-up actions 15](#_Toc180672152)

[Key considerations when setting up an internal whistleblowing system 17](#_Toc180672153)

[Scope 20](#_Toc180672154)

[What type of wrongdoing should be covered by internal whistleblowing systems? (material scope) 20](#_Toc180672155)

[Who should be able to report through your organisation’s IWS? (personal scope) 22](#_Toc180672156)

[Who should be protected? 22](#_Toc180672157)

[Roles and responsibilities 24](#_Toc180672158)

[Top leadership 24](#_Toc180672159)

[The whistleblowing officer or office 25](#_Toc180672160)

[Line managers 26](#_Toc180672161)

[Information and communication 27](#_Toc180672162)

[Informing your organisation’s personnel and other relevant stakeholders 27](#_Toc180672163)

[Information to provide 28](#_Toc180672164)

[Fostering a “speak up and listen up” culture 30](#_Toc180672165)

[Procedures 31](#_Toc180672166)

[Multiple whistleblowing channels 31](#_Toc180672167)

[Taking action on whistleblowing reports 32](#_Toc180672168)

[Record-keeping and data protection 37](#_Toc180672169)

[Support and protection for whistleblowers 39](#_Toc180672170)

[Protecting the identity of whistleblowers and other protected persons 39](#_Toc180672171)

[Protection from detrimental conduct and interference 40](#_Toc180672172)

[Addressing detrimental conduct, interference and breaches of confidentiality 43](#_Toc180672173)

[Supporting whistleblowers 45](#_Toc180672174)

[Protection of persons concerned 46](#_Toc180672175)

[Continuous monitoring, review and accountability 47](#_Toc180672176)

[Data collection 47](#_Toc180672177)

[Review and amendements 48](#_Toc180672178)

[Accountability to stakeholders 49](#_Toc180672179)

[Key principles for internal whistleblowing systems 51](#_Toc180672180)

# Acknowlegements

Transparency International would like to thank the following individuals and organisations who provided insight and expertise that greatly assisted the development of this self-assessment framework.

Alessia Rizzo, Transparency International Italia

Celine Pinzio, Transparency International

David Martinez, Transparency International España

Giorgio Fraschini, Transparency International Italia

Giovanni Pellerano, Whistleblowing Solutions

Ida Nowers, Transparency International Ireland

Irina Lonean, Transparency International Romania

Isabel Buechner, Transparency International

Jan Dupák, Transparency International Czechia

Judit Zeisler, Transparency International Hungary

John Devitt, Transparency International Ireland

Kremena Chobanova, Transparency International Bulgaria

Krista Asmusa, Transparency International Latvia (DELNA)

Kristina Marova, Transparency International Slovakia

Laurence Fabre, Transparency International France

Lousewies Van Der Laan, Transparency International Netherlands

Lotta Rydstrom, Transparency International Sweden

Lotte Rooijendijk, Transparency International Netherlands

Martim Agarez, Transparency International Portugal

Miklos Ligeti, Transparency International Hungary

Susanna Ferro, Whistleblowing Solutions

Zuzana Grochalová, Transparency International Slovakia

Protect, the UK’s whistleblowing charity

# Glossary

**Internal whistleblowing system**:an organisation’s whistleblowing-related objectives, policies, procedures, processes, guidelines and tools.

**Whistleblowing officer or office**: the person or department responsible for operation of the internal whistleblowing system.

**Whistleblowing**:communicating information on suspected wrongdoing (see below) to individuals or entities believed to be able to effect action.

**Wrongdoing**: an act or omission that is unlawful, abusive or can cause harm.

**Whistleblower**: any person reporting or disclosing information on suspected wrongdoing acquired in the context of their work-related activities, with the reasonable belief that the information reported was true at the time of reporting.

**Internal report**: a whistleblowing report made within a public or private organisation (i.e. within the workplace).

**External report**: a whistleblowing report made to a competent authority.

**Public disclosure**: making information on wrongdoing available in the public domain, either by publishing it – for example, on online platforms or social media – or reporting it to stakeholders such as the media, elected officials, civil society organisations, trade unions or business/professional organisations.

**Detrimental conduct**: any threatened, recommended or actual act or omission, direct or indirect, which causes or may cause harm, and is linked to or resulting from actual or suspected whistleblowing.

**Person concerned**: a natural or legal person referred to in a whistleblower’s report or complaint as a person responsible for the suspected wrongdoing or detrimental conduct, or associated with that person.

**Protected third parties**: persons other than a whistleblower at risk of detrimental conduct linked with whistleblowing.

**Personnel**:an organisation’s directors, officers, employees, temporary staff or workers, trainees and interns.

**Personnel representatives**: persons who are recognised as such under national law or practice, whether they are trade union representatives or elected representatives (e.g. works councils).

**Top management**: person or group of people who direct and control an organisation at the highest level (i.e. the executives).[[1]](#footnote-2)

**Governing body**: person or group of people who have ultimate accountability for a whole organisation.[[2]](#footnote-3)

# Acronyms

**CSO**: Civil society organisation

**CSR**: Corporate social responsibility

**DEI**: Diversity, equity and inclusion

**DPA**: Data protection agreement

**ESG**: Environmental, social and governance

**EU**: European Union

**GESI**: Gender, equality and social inclusion

**HR**: Human resources

**ISO:** International Organization for Standardization

**IWS**: Internal whistleblowing system

# Introduction

Whistleblowing is one of the most effective ways to uncover corruption, fraud, mismanagement and other wrongdoing that threatens public health and safety, financial integrity, human rights and the environment.

Whistleblowing is the disclosure of information about suspected wrongdoing to individuals or entities believed to be able to effect action. Organisations themselves are often best placed to deal with wrongdoing occurring within their remit, and in practice, most whistleblowers first report such suspected wrongdoing within their organisation. It is therefore essential that organisations, whether private companies or public institutions, provide safe and effective mechanisms to receive and address these reports, as well as robust protection to whistleblowers.

Consequently, an increasing number of national laws require organisations to implement an internal whistleblowing system (IWS), also known as “speak up” or internal reporting systems. This is the case, for example, in European Union (EU) countries, under the 2019 EU Whistleblower Protection Directive.

Organisations should view an IWS as more than just a legal requirement. An effective IWS not only safeguards the public interest, but also helps protect organisations from the repercussions of misconduct, such as legal liabilities, reputational damage and significant financial losses. As such, an IWS is considered essential in the context of environmental, social and governance (ESG) practices.[[3]](#footnote-4)

By enabling personnel and other relevant stakeholders to speak up about unethical or illegal conduct, an IWS fosters an organisational culture of trust, transparency and accountability. Such systems therefore provide real benefits to an organisation’s culture, brand, value creation and growth.[[4]](#footnote-5)

Transparency International has developed this self-assessment framework to support organisations in establishing, implementing and reviewing their internal whistleblowing systems, so that they are effective and in line with best practice and international standards, Transparency International’s [*IWS Best practice for public and private organisations*](https://www.transparency.org/en/publications/internal-whistleblowing-systems) and the ISO Guidelines for Whistleblowing Management Systems. While it is called a “self-assessment” framework, this tool can also be used by third party organisations, such as CSOs, authorities and consultancies, to conduct an in-depth assessment of an organisation’s IWS, either in collaboration with the organisation or based on publicly available data.[[5]](#footnote-6)

The framework is aimed at organisations across all sectors – public, private and “third” sectors – and jurisdictions, including international organisations, such as the United Nations. It also seeks to help organisations operating within the EU to meet their obligations under the EU Directive on Whistleblower Protection.

Organisations should use the self-assessment framework together with the above-mentioned principles and guidelines.

## Who should implement internal whistleblowing systems?

All public and most private organisations should have an internal whistleblowing system.

### All public organisations

All public entities, at local, regional, national or international level, without exception and regardless of size, should implement an IWS. This includes those that are publicly owned or controlled, such as state-owned enterprises.[[6]](#footnote-7) Entities should set up and implement an IWS in ways appropriate to their size and risk exposure. Small local authorities, such as municipalities, could share resources – for example, at the higher local level – for the receipt of reports and any subsequent investigation. However, the responsibility to maintain confidentiality, provide feedback to the whistleblower and address the reported wrongdoing remains with each organisation concerned.[[7]](#footnote-8)

### Most private organisations[[8]](#footnote-9)

* All medium-sized and large private entities with 50 or more employees should implement an IWS, as should all entities in the financial service industry, irrespective of size.[[9]](#footnote-10) This includes both companies and non-profit organisations.
* Small private entities with fewer than 50 employees are strongly advised to implement an IWS, especially when the nature of their activities exposes them to corruption risks or presents other risks to the public interest – for example, to human rights, the environment or public health. Companies that are part of a corporate group should have an IWS, regardless of their size.[[10]](#footnote-11)
* Small and medium-sized private entities with fewer than 250 employees could opt to share resources for the receipt of reports and any subsequent investigation. However, as in the public sector, the responsibility to maintain confidentiality, provide feedback to the whistleblower and address the reported wrongdoing remains with each organisation concerned.

Universal whistleblower protection

All entities, regardless of whether they have implemented a formal IWS, should have a zero-tolerance approach to detrimental conduct against whistleblowers. They should also facilitate reports of wrongdoing and act on concerns where possible.

|  |
| --- |
| THE EU WHISTLEBLOWER PROTECTION DIRECTIVE  In 2019, the European Union adopted the “Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law” (Whistleblower Protection Directive). The 27 EU member states had two years until December 2021 to comply with the directive, although most did not meet the deadline.[[11]](#footnote-12)  The directive provides strong common minimum standards for the protection of whistleblowers in Europe. Member states are required to transpose these provisions in line with the spirit of the directive, which is to provide a high level of protection for whistleblowers.  **Key provisions of the EU Whistleblower Directive**:   * The directive covers both the public and private sectors. * It covers a wide range of potential whistleblowers, including individuals outside the traditional employee-employer relationship, such as consultants, contractors and volunteers; persons belonging to the administrative, management or supervisory body; former workers and job applicants (Article 4). * It also protects individuals who assist whistleblowers, as well as individuals and legal entities connected with whistleblowers (Article 4.4). * Breaches of law are defined as acts or omissions that are either unlawful or that defeat the object or the purpose of the rules (Article 5.1). * In granting protection, the directive does not in any way take into account the whistleblower’s motive for reporting. * It protects the identity of whistleblowers in most circumstances, with clear and limited exceptions to confidentiality, and advance notice to the whistleblower when their identity needs to be disclosed (Article 16). * It grants protection to whistleblowers who have reported or disclosed information anonymously and have subsequently been identified (Article 6.3). * It places an obligation on a wide range of public and private entities to establish internal whistleblowing systems (Article 8). * Public and private entities and competent authorities are obliged to follow up on reports received and to keep the whistleblower informed within a reasonable timeframe (Articles 9 and 11.2). * The directive allows whistleblowers to report breaches of law internally or directly to the competent authorities (Article 10). * It allows for public disclosures in certain circumstances (Article 15). * It prohibits “any form of retaliation”, including threats of retaliation and attempts at retaliation, and provides a long, diverse and non-exhaustive list of examples (Article 19). * EU member states are required to ensure that easily accessible and free, comprehensive and independent advice is provided to the public (Article 20.1(a)). * The directive foresees legal and financial assistance to whistleblowers, which are essential elements of effective whistleblower protection (Article 20.2). * It creates a presumption of retaliation when a whistleblower suffers detriment (Article 21.5). * It provides for interim relief which enables a whistleblower to maintain professional and financial status until legal proceedings end (Article 21.6). * The directive provides for penalties to be applied to persons who hinder or attempt to hinder reporting, retaliate against whistleblowers (including by bringing vexatious proceedings) or breach the duty of maintaining confidentiality over the whistleblower’s identity (Article 23). * It provides that whistleblowers cannot be held liable for breaching restrictions on the acquisition or disclosure of information, including for breaches of trade or other secrets (Article 21(2)(3)(7)). It also excludes the possibility of contracting out of the right to blow the whistle – for example, through loyalty clauses, or confidentiality or non-disclosure agreements (Article 24). |

# Conducting the self-assessment

The self-assessment framework should be administered as a crucial step in designing or reviewing an organisation’s Internal Whistleblowing System (IWS). Using the self-assessment framework is essential for several reasons:

* **Identifying strengths and weaknesses**: The framework helps organisations evaluate the effectiveness of their IWS. By identifying strengths and weaknesses, organisations can reinforce good practices and address gaps, to improve overall effectiveness.
* **Ensuring best practices**: Findings from the framework help ensure that an organisation adheres to best practices related to whistleblower protection. This is crucial for maintaining trust from personnel and stakeholders, and fostering an environment that encourages ethical reporting.
* **Promoting a culture of transparency and accountability**: The process encourages a culture where personnel feel safe to report wrongdoing without fear of retaliation. It demonstrates an organisation's commitment to transparency, integrity and ethical behaviour, fostering trust among personnel.
* **Guiding improvements and reforms**: The insights gained from the framework can guide targeted reforms and improvements in the whistleblowing procedures. These can include updating policies, improving communication strategies, or enhancing training programmes to better support potential whistleblowers.
* **Facilitating internal communication and collaboration**: Involving different departments, such as human resources and compliance, in the self-assessment promotes internal communication and collaboration. It ensures a more comprehensive understanding of the whistleblowing process and integrates feedback from various perspectives within an organisation.
* **Enhancing organisational learning**: Regular self-assessment provides opportunities for continuous learning and development. It helps your organisation stay updated on best practices, adapt to new expectations, and respond effectively to emerging challenges in whistleblower protection.
* **Building trust with external stakeholders**: By demonstrating a commitment to self-evaluation and improvement, your organisation builds trust with external stakeholders, including regulators, partners and the public. This trust is critical for maintaining a positive reputation and ensuring long-term sustainability.

Overall, using the self-assessment framework is a proactive measure to enhance the effectiveness of an organisation’s whistleblowing system, protect whistleblowers and uphold ethical standards.

## Roles and responsibilities in conducting the assessment

The whistleblowing officer or office is responsible for conducting the self-assessment. To maximise its effectiveness, they should collaborate with other departments or functions, such as Human Resources (HR), Compliance, Ethics, Legal, Corporate Social Responsibility (CSR) and Diversity, Equity and Inclusion (DEI), as well as relevant bodies, including the governing body and personnel representatives. These groups can provide input for specific questions and contribute to the analysis of responses and discussions on the next steps.

If your organisation does not yet have designated a whistleblowing officer of office, other functions, such as compliance, governance or audit, can conduct the self-assessment. It is generally advised that the self-assessment task is not assigned to HR or management, due to potential conflicts of interest. Both HR and management are often directly involved in handling sensitive personnel issues and overseeing employees, which could create bias or affect objectivity in the assessment process.

Assigning the task to independent functions such as compliance, governance or audit ensures a more impartial review. These departments typically operate with a degree of separation from day-to-day personnel decisions, making them better suited to assessing the IWS objectively, ensuring integrity and promoting trust in the process.

## Assessment framework: dimensions and questions

The core of the assessment is structured around a set of 130 questions clustered under eight dimensions and divided into 20 sub-categories, as described in the table below:

|  |  |
| --- | --- |
| **Dimensions** | **Sub-categories** |
| Key considerations when setting up an IWS | *Gender, equality and social inclusion in IWS* |
| Scope | What type of wrongdoing should be covered by internal whistleblowing systems?  Who should be able to report through internal whistleblowing systems?  Who should be protected? |
| Roles and responsibilities | Top leadership  The whistleblowing officer or office  Line managers |
| Information and communication | Provision of information to all relevant stakeholders  Information to provide  Fostering a “speak up and listen up” culture |
| Procedures | Multiple whistleblowing channels  If outsourcing to external service providers  Taking action on whistleblowing reports  Record-keeping and data protection |
| Support and protection for whistleblowers | Protecting the identity of whistleblowers and other protected persons  Protection from detrimental conduct and interference  Addressing detrimental conduct, interference and breaches of confidentiality  Supporting whistleblowers |
| Protection of persons concerned | Protection of persons concerned |
| Continuous monitoring and review | Data collection  Review and amendments  Accountability to stakeholders |

The structure of the framework largely mirrors the structure of Transparency International’s [*IWS Best practice for public and private organisations*](https://www.transparency.org/en/publications/internal-whistleblowing-systems)*,* for ease of reference.

## Instructions for Completing the framework

Each question can be answered with ”yes”, “no” or “partially”. Some questions consist of multiple components, including follow-up or detailed questions, while others may have sub-questions. Users should answer “yes” or “no” only if this answer applies to all elements of the question. If some elements of the question require yes” and others “no”, then the response should be “partially”.

|  |
| --- |
| Sample question that could be answered by “partially”  1. In addition to employees, can any person with a work-related relationship with your organisation report wrongdoing covered by the organisation’s IWS (thereafter “relevant wrongdoing”)? This includes at least the following categories of individuals, whether their relationship with your organisation is current or has ended:    * workers (whether full- or part-time, fixed-term or temporary), including civil servants    * self-employed persons    * shareholders and persons belonging to the administrative, management or supervisory body    * volunteers and paid or unpaid trainees    * persons working under the supervision and direction of contractors, sub-contractors and suppliers    * persons such as job applicants or bidders who acquired information during the recruitment process or other pre-contractual negotiations.   This question should be answered “partially” if one or more of the categories of persons listed cannot report relevant wrongdoing through your organisation’s IWS – for example, if volunteers are not able to report relevant wrongdoing through the IWS. |

Users should also answer “partially” in cases where there is only an informal practice in place, and it is not formally established through an official policy, procedure, process or guideline.

For organisations that have already been implementing an IWS for some time, users are invited to base their responses on the actual outcomes and effectiveness of the system, where applicable, rather than solely on the existence or not of specific measures.

If a question is answered “no” or “partially”, users should note the reasons in the comments section. This section should also be used to propose potential ways to address the gaps identified.

### Data sources

To complete the framework, users will need to refer to several data sources, including:

* the organisation’s whistleblowing policy
* procedures for handling whistleblowing reports
* data on whistleblowing and retaliation cases
* risk registers and compliance risk assessments
* audit results or other evaluations related to governance, compliance and organisational culture
* other relevant policies, such as those on sexual harassment and bullying, grievances and data protection, and the organisational code of conduct
* standing agendas from governing and other oversight bodies, specifically checking for inclusion of the IWS or related reporting
* surveys of personnel
* training curriculums
* data on all wrongdoing, whether reported by a whistleblower, or detected by other means (e.g. audit)
* leaflets, internal newsletters and relevant sections of the organisation’s intranet and website
* templates for employment and supplier contracts.

## Analysing the answers and defining follow-up actions

After all the questions have been answered and the IWS strengths and weaknesses identified and documented in the comments section, the next step is to develop specific recommendations for improving the IWS. It is advisable to formulate recommendations for each identified gap or weakness before deciding on any prioritisation.

When formulating recommendations to improve areas that have received answers of “no” or “partially”, we encourage users to consult Transparency International’s *IWS Best Practice Principles for public and private organisations*. This self-assessment framework has been designed as a complementary tool to the IWS Best Practice Principles, and follows the same structure, making it easier for users to locate the relevant principles and guidance when looking to enhance specific aspects of their IWS.

The self-assessment framework does not assign a score or give more weight to specific questions, sub-sections or dimensions. Therefore, users should not assume that a sub-section or dimension is “sufficiently strong” and does not require further improvement just because most of the questions in it were answered “yes”.

The whistleblowing officer or office should invite relevant departments and bodies, such as HR, Compliance, Ethics, Legal and DEI, as well as the governing body and personnel representatives, to contribute to the analysis of responses, the development of recommendations and discussions on the next steps.

Follow-up actions might include revising relevant policies, procedures and processes; updating training content and information provided to personnel; launching an internal awareness-raising campaign, and amending employment and external service contract templates.

# Key considerations when setting up an internal whistleblowing system

| **Questions** | | **Y** | **N** | **P[[12]](#footnote-13)\*** |
| --- | --- | --- | --- | --- |
| 1 | Has your organisation undertaken a comprehensive risk and needs assessment to inform the design of its IWS? |  |  |  |
| 2 | Has the IWS been designed following consultation with relevant stakeholders, including personnel, works councils, trade unions or other personnel representatives, and – where appropriate – in agreement with them? |  |  |  |
| 3 | Has your organisation ensured compliance of its IWS with national legal requirements, under whistleblower protection legislation and other legislation, such as data protection, labour, anti-money laundering and anti-bribery laws? |  |  |  |
| 4 | Is the IWS part of the organisation’s governance framework and linked to integrity and compliance programmes? |  |  |  |
| 5 | Has your organisation implemented measures to make its whistleblowing policy legally binding between the organisation and its employees, ensuring whistleblower protection as outlined in the policy, particularly when such protection exceeds the safeguards provided by national law?  ***Note:*** National legal requirements applicable to an IWS often fail to meet best practice in one or more areas, such as the material and personal scope, anonymous reporting, protection and support measures, and restorative actions. An organisation should always provide clear information on the applicable law, including who is protected by national whistleblower protection legislation, for what, and how. If your organisation’s IWS goes beyond legal requirements in one or more areas, the organisation should highlight differences between the IWS and the law, so that potential whistleblowers understand what constitutes their legal protection and what is a voluntary higher commitment by the organisation. In addition, your organisation should stress that while it can provide comprehensive protection from detrimental conduct against the whistleblower in the workplace, its capacity to protect whistleblowers outside the workplace is limited. |  |  |  |
| 6 | Is your organisation clear about how it will distinguish internal whistleblowing from other types of feedback and complaints, such as grievances? |  |  |  |
| 7 | Has the IWS been designed following consultation with relevant stakeholders, including personnel, works councils, trade unions or other personnel representatives, and – where appropriate – in agreement with them? |  |  |  |
| 8 | Has your organisation considered accessibility, gender-sensitivity and inclusiveness when designing its IWS? |  |  |  |
| 9 | If your organisation is part of a group, network or partnership, have you considered aligning your IWS with that of other member organisations, particularly with that of the headquarters or equivalent entity, as well as how your organisation’s IWS integrates with those systems? This applies, for example, to companies within a corporate group, CSOs in a formal network, or members of a partnership organisation. |  |  |  |
| 10 | If your organisation is the headquarters or equivalent entity of a group, network or partnership, is it taking measures to support member organisations to implement an IWS that is effective, and to facilitate alignment of these systems with your organisation’s IWS – for example, by providing guidelines, training or a platform? |  |  |  |
| **Comments and recommendations:** | | | | |

|  |
| --- |
| GENDER, EQUALITY AND SOCIAL INCLUSION IN AN IWS  An IWS that is sensitive to issues of gender, equality and social inclusion (GESI) aims to create an inclusive and accessible environment for all potential whistleblowers, promoting a culture where everyone feels confident to report wrongdoing without fear of retaliation or discrimination. To develop and implement a GESI-sensitive IWS effectively, organisations should take into account:   * **Whistleblowing policy**: Does your organisation’s whistleblowing policy explicitly mention gender equality and social inclusion principles? * **IWS scope**: Does the IWS cover gender-based violence, harassment, discrimination, bullying and other forms of workplace misconduct that disproportionately affect marginalised groups? * **Reporting channels**: Are various confidential and anonymous reporting channels accessible to all potential whistleblowers, and do they take into consideration factors such as language barriers, gender, illiteracy, disabilities, cultural sensitivity, limited access to technology, and people’s need to be able to submit reports within and outside regular working hours? * **Accessibility of information**:Is information about the IWS available in clear, easily accessible and inclusive language, as well as in multiple languages where appropriate? Has your organisation ensured that information about its IWS is disseminated in ways that are inclusive, gender-sensitive and accessible for persons with disabilities? * **Training**:Does your organisation provide specific training for managers, whistleblowing officers and investigators on handling reports involving marginalised groups in a sensitive and impartial manner? * **Support**:Does your organisation offer support services to whistleblowers, such as access to psychological support, confidential counselling, legal assistance and whistleblower peer support networks, with a focus on those who may face additional challenges due to their social identity, such as gender, race, ethnicity, age, socioeconomic status, sexual orientation or disability? * **Diverse whistleblowing and investigation teams**: Do the criteria for designation of the persons responsible for handling reports ensure inclusiveness and gender sensitivity? * **Data collection and analysis**: Does your organisation collect and analyse anonymised, disaggregated data to identify and address reporting patterns and barriers, including detrimental conduct, taking into account gender and other factors that influence individual experiences, such as race, ethnicity or disability? * **Reviews**: Do reviews involve relevant stakeholders, including personnel representatives, the DEI office or officer, the governing body, and relevant departments, such as HR, Compliance, Ethics and Legal? * **Stakeholder engagement**: Does your organisation engage with civil society organisations and GESI experts to continually improve the IWS and ensure it remains relevant and inclusive?   *Note: these questions are integrated into the relevant sections of the framework.* |

# Scope

Does your organisation clearly define who can report and what can be reported – and addressed – through its IWS, as well as who is protected?

| **Questions** | | **Y** | **N** | **P[[13]](#footnote-14)\*** |
| --- | --- | --- | --- | --- |
| What type of wrongdoing should be covered by internal whistleblowing systems? (material scope) | | | | |
| 11 | Does the IWS define wrongdoing as any act or omission that is unlawful, abusive or can cause harm? Does its scope cover any suspected wrongdoing falling within that definition and that is, has been or is likely to be committed in, by or for the organisation? Note that IWS scope potentially goes beyond minimum legal requirements. |  |  |  |
| 12 | If not, does the IWS cover at least the following:   * criminal offences * breaches of legal obligations (national and international) * dangers to public and occupational health and safety * dangers to the environment * human rights violations * child exploitation or abuse * gender-based violence, harassment, bullying and discrimination * corruption in all its forms, including bribery, money laundering, sexual corruption, embezzlement, misappropriation, abuse of authority, obstruction of justice and illicit enrichment * other breaches of ESG standards * insider trading, tax evasion or breaches of antitrust law and international trade sanctions * conflicts of interest * fraudulent financial disclosures * gross waste or mismanagement * detrimental conduct against whistleblowers and other protected parties * conduct that involves significant risk to your organisation because it is harmful to its interests, reputation, operations, financial wellbeing or governance, as well as any other violation of your organisation’s codes of conduct or ethics, and relevant policies * concealment of wrongdoing and attempts to conceal such wrongdoing, including interfering or attempting to interfere with whistleblowing? |  |  |  |
| 13 | Does the IWS scope cover suspected wrongdoing that is, has been or is likely to be committed in, by or for the organisation? This means wrongdoing committed by personnel, but also by any person working directly or indirectly for the organisation, including current and former personnel; persons belonging to the administrative, management or supervisory body; volunteers, contractors or sub-contractors, and suppliers or consultants, in the context of their work for the organisation? |  |  |  |
| **Comments and recommendations:** | | | | |
| Who should be able to report through your organisation’s IWS? (personal scope) | | | | |
| 14 | In addition to employees, can any person with a work-based relationship with the organisation report wrongdoing covered by its IWS (thereafter “relevant wrongdoing”)?[[14]](#footnote-15) This includes at least the following categories of individual, whether their relationship with the organisation is current or has ended:   * workers (whether full- or part-time, fixed-term or temporary), including civil servants * self-employed persons * shareholders and persons belonging to the administrative, management or supervisory body * volunteers and paid or unpaid trainees * persons working under the supervision and direction of contractors, sub-contractors and suppliers * persons such as job applicants or bidders, who acquired information during the recruitment process or other pre-contractual negotiations? |  |  |  |
| **Comments and recommendations:** | | | | |
| Who should be protected? | | | | |
| 15 | Does the IWS define “whistleblowers” as any persons who report, attempt to report, are believed to be about to report, or are believed to have reported suspected wrongdoing with the reasonable belief that the information reported was true at the time of reporting? |  |  |  |
| 16 | If a person claims that the reporting person – presumed whistleblower – knew the information was false at the time of reporting, does the IWS place the burden to prove it on the person making that claim? Does the IWS have a process for handling knowingly false reports and for warning reporting persons that if they make a knowingly false report, they will not be afforded protection and may face legal penalties? |  |  |  |
| 17 | Does the IWS avoid using terminology describing the reporting person’s motive, such as “in good faith”, “malicious”, “vexatious” or “abusive”? |  |  |  |
| 18 | Does the IWS protect whistleblowers whether they reported internally or externally to the authorities, or made a public disclosure in line with legislation? |  |  |  |
| 19 | Does the IWS protect whistleblowers who reported information on wrongdoing anonymously – internally, externally or via public disclosure – and are subsequently identified? |  |  |  |
| 20 | Does the IWS protect whistleblowers whether they used the designated internal channels or reported to another “natural” internal authority, such as a manager, health and safety officer, chief compliance officer, HR officer, integrity officer, legal or privacy officer, chief financial officer, chief audit executive or member of the governing body? |  |  |  |
| 21 | Does the IWS cover individuals who have a professional obligation to report wrongdoing in the course of their job duties, such as internal auditors or health and safety officers? |  |  |  |
| 22 | Does your organisation protect third parties at risk of detrimental conduct? These include:   * legal entities that the whistleblower owns, works for or is otherwise connected with * third parties connected with the whistleblower, such as colleagues and relatives * naturalpersons who assist or attempt to assist a whistleblower, in a confidential manner * legal persons, including civil society organisations (CSOs) and trade unions, who assist or attempt to assist a whistleblower, in a confidential manner * persons named in the report as potential witnesses * persons participating in the follow-up of a report, including witnesses * persons who refuse to participate in wrongdoing. |  |  |  |
| **Comments and recommendations:** | | | | |

# Roles and responsibilities

Does your organisation clearly establish and communicate roles and responsibilities of all those involved in the implementation of its IWS?

| **Questions** | | **Y** | **N** | **P[[15]](#footnote-16)\*** |
| --- | --- | --- | --- | --- |
| Top leadership | | | | |
| 23 | Has the IWS been approved by your organisation’s top management and its highest oversight body (hereafter “the governing body”)? |  |  |  |
| 24 | Does the IWS designate the governing body as responsible for ultimate oversight of the whistleblowing system? |  |  |  |
| 25 | Have your organisation’s top management and governing body ensured that the IWS is adequately resourced to fulfil its objectives effectively? |  |  |  |
| 26 | Are your organisation’s top management and governing body properly trained or, at a minimum, briefed to understand the importance of the IWS, its operation and their roles in supporting it? |  |  |  |
| **Comments and recommendations:** | | | | |
| The whistleblowing officer or office | | | | |
| 27 | Based on its size, risk exposure and needs, has your organisation designated a person (the “whistleblowing officer”) or department (the “whistleblowing office”) as responsible for the operation of the IWS, including for:   * designing, monitoring and reviewing the IWS * providing information on the IWS to any person * receiving, assessing, following up and providing feedback on reports * assessing and monitoring risks of retaliation against whistleblowers * receiving, assessing, following up and providing feedback on retaliation complaints from whistleblowers * regularly reporting to your organisation’s top management and governing body on implementation of the IWS? |  |  |  |
| 28 | Does the whistleblowing officer or head of the whistleblowing office have direct and ready access to the governing body that oversees the IWS? |  |  |  |
| 29 | Is the whistleblowing officer or head of the whistleblowing office afforded sufficient independence and authority through the organisational or governance structure? |  |  |  |
| 30 | Does the IWS provide solutions for potential conflicts of interest of the whistleblowing officer or office? |  |  |  |
| 31 | Does the whistleblowing officer or do members of the whistleblowing office have the relevant qualifications and receive specific and regular training for the purpose of operating the IWS, including to ensure inclusiveness and gender sensitivity in its implementation? |  |  |  |
| 32 | Do the criteria for designation of the persons responsible for handling reports ensure inclusiveness and gender sensitivity? |  |  |  |
| **Comments and recommendations:** | | | | |
| Line managers | | | | |
| 33 | Does the IWS protect whistleblowers reporting to line managers? |  |  |  |
| 34 | Are line managers regularly trained – at least once a year – in the receipt and handling of whistleblowing reports, addressing issues including the scope of the IWS and the legal framework, how to recognise whistleblowing reports, how to handle the information received – such as referring the whistleblower to the relevant channels, maintaining confidentiality – and how to handle situations involving marginalised groups, gender-based violence, harassment or discrimination with sensitivity and impartiality? |  |  |  |
| **Comments and recommendations:** | | | | |

# Information and communication

Does your organisation provide information about its IWS to all relevant stakeholders, to ensure awareness?

| **Questions** | | **Y** | **N** | **P[[16]](#footnote-17)\*** |
| --- | --- | --- | --- | --- |
| Informing your organisation’s personnel and other relevant stakeholders | | | | |
| 35 | Is the IWS signposted internally, through the channels most commonly used by personnel, such as leaflets, posters or your organisation’s intranet, and in languages that allow access to all? |  |  |  |
| 36 | Does your organisation provide information about the IWS on its website, in a dedicated, easily accessible section, and in languages that allow access to all, so as to reach relevant stakeholders other than personnel? |  |  |  |
| 37 | Does your organisation provide awareness training to all personnel, at induction and at regular intervals? |  |  |  |
| 38 | Does your organisation regularly promote its IWS internally – for example, at general personnel meetings, in internal newsletters or via email? |  |  |  |
| 39 | Do your organisation’s contract templates – including for employment, supply, consultancy and service provision – require the signatory to read and acknowledge the organisation’s code of conduct and whistleblowing policy? |  |  |  |
| 40 | Has your organisation ensured that the dissemination channels for information on its IWS are inclusive, gender-sensitive and accessible to persons with disabilities? |  |  |  |
| 41 | Does your organisation provide safe ways for personnel and other stakeholders covered by the IWS to receive comprehensive information and guidance on its scope and procedures, the protection against detrimental conduct, available remedies and the rights of persons concerned (i.e. the persons referred to in a whistleblower’s report as responsible for the suspected wrongdoing or detrimental conduct)? |  |  |  |
| **Comments and recommendations:** | | | | |
| Information to provide | | | | |
| 42 | Does your organisation provide information about:   * roles and responsibilities related to the IWS, including who is accountable for it * the scope of the IWS, including in relation to other internal reporting or complaint systems, such as grievance mechanisms, with guidance about which reporting or complaint system is best suited to receive and handle which types of concern * the conditions for qualifying for protection under the IWS, making it clear that:   + a person’s motives for reporting suspected wrongdoing are irrelevant to their protection, as long as they reasonably believe that the information reported was true at the time of reporting   + whistleblowers are protected regardless of whether subsequent investigation finds proof of wrongdoing, including those who reported inaccurate information in honest error * the applicable law, including who is protected by national whistleblower protection legislation and how, highlighting potential differences between the organisation’s whistleblowing and whistleblower protection policy and procedures, and the law, so that potential whistleblowers understand what constitutes their legal protection and what is a voluntary higher commitment by your organisation * contact details for the internal information and reporting channels * the procedures applicable to the reporting of wrongdoing, including for:   + requests for clarification or further information   + acknowledgement of receipt   + feedback to the whistleblower   + the nature of the follow-up, including main steps – such as initial assessment, investigation, closure of the case – and corresponding timeframe * the confidentiality and anonymity regime, including legal exceptions and practical limitations * the type of protection and support measures your organisation provides to whistleblowers, including the procedures and remedies to address detrimental conduct * how personal data will be processed, how long it will be retained and for what purpose * confidential, independent advice channels available outside the organisation, free of charge, such as those run by national authorities, trade unions or CSOs * the procedures for reporting externally to competent authorities?[[17]](#footnote-18) |  |  |  |
| 43 | Does the IWS clearly state that personnel are prohibited from engaging in any form of detrimental conduct against a whistleblower or protected third party, and that such behaviour will be subject to disciplinary action? |  |  |  |
| 44 | Does the IWS clearly state that where a report is received through internal channels other than the designated reporting channels, or by personnel other than those responsible for handling reports, the person who receives the report is prohibited from disclosing any information that might identify the whistleblower or the persons concerned, and should promptly direct the whistleblower to the proper channel, where possible? |  |  |  |
| 45 | Does the IWS explain that the protection offered by confidentiality or anonymity is not absolute in practice? For example, if your organisation is very small, or the whistleblower is the only witness or has mentioned their concerns to colleagues before making a report, there is a risk that the report will be traced back to them. |  |  |  |
| **Comments and recommendations:** | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Questions** | | **Y** | **N** | **P[[18]](#footnote-19)\*** |
| Fostering a “speak up and listen up” culture | | | | |
| 46 | Does the IWS reflect and reinforce your organisation’s values? |  |  |  |
| 47 | Does your organisation invite its stakeholders to discuss ethically challenging situations openly? |  |  |  |
| 48 | Does your organisation monitor its “speak up and listen up” culture – for example, via surveys and other feedback mechanisms? Are results from monitoring activities used to continuously improve policies and practices? |  |  |  |
| 49 | Is your organisation’s leadership perceived by internal and external stakeholders as ethical and supportive of the IWS? This perception may be measured through stakeholder engagement surveys and personnel feedback. |  |  |  |
| 50 | Does your organisation’s top leadership promote the IWS as a key element of governance and a tool for continuous improvement? This includes providing clear, consistent and supportive communication in writing and in person, both internally to personnel, and externally to other stakeholders and the general public. |  |  |  |
| 51 | Do all levels of management and all direct supervisors express support for the IWS – for example, by encouraging staff to attend training on the IWS? |  |  |  |
| 52 | Are line managers held accountable for promoting and upholding a culture of integrity and ethical conduct, including for fostering a speak-up culture – for example, by inclusion of this as an aspect of their performance review? |  |  |  |
| 53 | Does your organisation commend whistleblowers for speaking up, including through private or – with the whistleblower’s consent – public recognition from senior management? |  |  |  |
| 54 | Are the persons responsible for receiving reports and communicating with the whistleblower – such as the whistleblowing officer, line managers or an external service provider – trained in how to listen and to create psychological safety? |  |  |  |
| **Comments and recommendations:** | | | | |

# Procedures

Has your organisation implemented systems to receive and follow up on whistleblowing reports?

| **Questions** | | **Y** | **N** | **P[[19]](#footnote-20)\*** |
| --- | --- | --- | --- | --- |
| Multiple whistleblowing channels | | | | |
| 55 | Does your organisation provide multiple whistleblowing channels, enabling reporting in writing and orally, online, offline and remotely, which are easily accessible to personnel and other stakeholders covered by the organisation’s IWS – such as email, web-based platform, telephone, post, physical meetings and “letter boxes”?[[20]](#footnote-21) |  |  |  |
| 56 | When setting up its whistleblowing channels, has your organisation considered and addressed factors such as language barriers, gender, illiteracy, disabilities, limited access to technology, and people’s need to be able to submit reports within and outside regular working hours? |  |  |  |
| 57 | Are your organisation’s internal whistleblowing channels operated only by designated persons or other appropriate persons?[[21]](#footnote-22) |  |  |  |
| 58 | Does your organisation have a whistleblowing channel that enables anonymous reporting? |  |  |  |
| 59 | Does your organisation provide safe communication channels between the whistleblower – including those who are anonymous, where applicable – and the person handling their report, which allow the transfer of supporting documents in both physical and digital forms? |  |  |  |
| 60 | Does your organisation recognise line managers as possible recipients of internal whistleblowing reports? |  |  |  |
| **Comments and recommendations**: | | | | |
| If your organisation is outsourcing reporting channels to external service providers | | | | |
| 61 | Does your organisation remain in charge of following up on the report, addressing identified wrongdoing and providing feedback to the whistleblower? |  |  |  |
| 62 | Has your organisation ensured that the external service provider complies with the legal and best-practice requirements applicable to an IWS? Are guarantees of independence and confidentiality reflected in the service contract? |  |  |  |
| 63 | Are the role, tasks and responsibilities of the external provider clearly established and communicated to personnel and other stakeholders covered by your organisation’s IWS? |  |  |  |
| **Comments and recommendations**: | | | | |

| **Questions** | | **Y** | **N** | **P[[22]](#footnote-23)\*** |
| --- | --- | --- | --- | --- |
| Taking action on whistleblowing reports | | | | |
| 64 | Does your organisation’s IWS ensure thorough, timely follow-up of whistleblowing reports, including of anonymous reports where possible? |  |  |  |
| 65 | Does the follow-up involve a defined process for receipt of reports and their initial assessment, investigation and closure – with clear criteria for taking decisions at the end of each step? |  |  |  |
| 66 | Is the report follow-up carried out under strict confidentiality rules, on a need-to-know basis? |  |  |  |
| 67 | Does your organisation operate a case management system for the recording, follow-up and monitoring of whistleblowing reports and complaints of retaliation? |  |  |  |
| 68 | Do failures by the person responsible to acknowledge receipt of a report, follow up on a report or provide feedback to a whistleblower trigger an investigation, with potential disciplinary action for misconduct or failure to perform duty, where appropriate? |  |  |  |
| 69 | Does the IWS provide whistleblowers, protected third parties and persons concerned with a system to appeal for a review decisions concerning a) closure of the case or referral to another procedure, b) the conduct or outcome of any follow-up or investigation actions, c) the conduct or outcome of any investigation of a complaint of retaliation, or d) any decision to disclose the identity of a reporting person (except in exceptional cases)? |  |  |  |
| **Comments and recommendations:** | | | | |
| Communication with whistleblowers, and their participation | | | | |
| 70 | Does communication with whistleblowers take place regularly throughout the follow-up process, allowing them to clarify their report, provide additional evidence, and share concerns about risks of detrimental conduct and identity protection? Can the whistleblower decline further communication? |  |  |  |
| Acknowledgement of receipt | | | | |
| 71 | Is an acknowledgement of receipt of a report provided to whistleblowers within a short, pre-established timeframe,[[23]](#footnote-24) and does it include the following:   * opportunity for the whistleblower to clarify their report and provide additional information or evidence * the timeframe for further contact * the whistleblower’s responsibilities, such as maintaining confidentiality, and not investigating the suspected wrongdoing themselves * the advice and support measures available and the process for reporting detrimental conduct * relevant IWS material and policies? |  |  |  |
| Feedback to whistleblowers | | | | |
| 72 | Is feedback provided to the whistleblower regularly, at a minimum at the following times:   * at completion of the initial assessment of the report, and no later than within three months of receipt of the report – whichever comes first * at the main steps in the follow-up process and at least every three months * at the closure of the follow-up process? |  |  |  |
| 73 | Does regular feedbackto the whistleblower include information on:   * whether the report will be further followed up and, if not, an explanation why – for example, the report is outside the IWS scope, or there is not enough evidence * the anticipated timeframe for follow-up of the report * the actions envisaged or taken as follow-up to the report, and their grounds * measures taken to protect the whistleblower’s identity or anonymity; the available support and, where relevant, measures taken to protect them against detrimental conduct * when the whistleblower can expect further feedback on the follow-up to their report? |  |  |  |
| 74 | Are whistleblowers informed of the findings and outcome of the follow-up to their report, including information on:   * which allegations were investigated, and any significant limitations to the investigation * conclusions reached for each allegation * an outline of corrective measures * where relevant, an explanation of any limitation to the information that can be provided? |  |  |  |
| 75 | Are whistleblowers given the opportunity to review and provide comments on these results, and are their comments included in the follow-up report? |  |  |  |
| **Comments and recommendations**: | | | | |
| Initial assessment of whistleblowing reports | | | | |
| 76 | Are all received reports recorded, acknowledged and assessed diligently, including the possibility for the person following up on the report to ask further information from the whistleblower? |  |  |  |
| 77 | On receipt of the report, does the person handling it conduct an initial assessment of the risk of detrimental conduct against the whistleblower?[[24]](#footnote-25) |  |  |  |
| 78 | On receipt of the report, does the person handling it assess risks of harm to other parties, your organisation itself and the public interest, and repeat the assessment regularly throughout the follow-up process? |  |  |  |
| 79 | Can your organisation take support and protection measures to prevent detrimental conduct and harm to the whistleblower, other parties, the organisation itself and the public interest, on recommendation of the whistleblowing officer? |  |  |  |
| 80 | Where a report is found to be beyond the scope of the IWS, is the whistleblower directed to another internal reporting or complaint system, or possibly to one outside your organisation, where available? |  |  |  |
| **Comments and recommendations**: | | | | |
| Investigation of reported wrongdoing | | | | |
| 81 | Does your organisation have investigation protocols that ensure due process, including:   * respect for the presumption of innocence of persons concerned and their rights to respond and receive assistance during the follow-up process * measures to ensure that the person following up on the report can carry out or oversee the investigation with sufficient independence from the whistleblower, persons concerned and other interested parties? |  |  |  |
| 82 | For each investigation, are clear terms of reference developed, which identify the scope, methods, skills and resources required? |  |  |  |
| 83 | Do investigations observe “victim/survivor-focused” principles when appropriate, such as in cases of bullying, sexual harassment, sexual corruption or sexual exploitation, and are they conducted in a way that avoids re-traumatisation and prioritises the wellbeing, needs and wishes of the victims? |  |  |  |
| 84 | Are risks of detrimental conduct against the whistleblower and other protected parties monitored throughout the follow-up process? |  |  |  |
| 85 | Are preliminary investigation findings presented to the whistleblower for their review and potential comments, and are any such comments included in the investigation report? |  |  |  |
| **Comments and recommendations**: | | | | |
| Closure of follow-up | | | | |
| 86 | Does the IWS specify that if an investigation found that wrongdoing is occurring, has occurred or is likely to occur, your organisation should take the necessary action to address it, including, as appropriate, measures to:   * stop or prevent the wrongdoing and minimise its effects * sanction the perpetrators of the wrongdoing, where identified * remedy any damage caused * report to the competent authorities? |  |  |  |
| 87 | Does the IWS specify that your organisation should take appropriate action to correct any systemic issue identified, such as weaknesses in policy, procedure or controls, whether or not the investigation revealed wrongdoing? |  |  |  |
| 88 | Does the IWS allow for cases to be re-opened where new information that warrants continued investigation is shared – for example, by the whistleblower or another whistleblower? |  |  |  |
| 89 | Does the whistleblowing officer or office continue to monitor risks of detrimental conduct against the whistleblower after closure of the follow-up? |  |  |  |
| **Comments and recommendations**: | | | | |

| **Questions** | | **Y** | **N** | **P[[25]](#footnote-26)\*** |
| --- | --- | --- | --- | --- |
| Record-keeping and data protection | | | | |
| 90 | Does your organisation document reports received, actions taken as follow-up, and the findings and outcome of the follow-up, as well as communication with the whistleblower and person concerned, in a way that guarantees the confidentiality of the report and, where appropriate, the whistleblower’s anonymity? |  |  |  |
| 91 | Are reports stored for a proportionate amount of time and no longer than necessary, including to allow for their diligent follow-up and for the protection of whistleblowers against detrimental conduct, and of the rights of the person concerned? |  |  |  |
| 92 | Are those records kept in retrievable and auditable form, in accordance with confidentiality and data-protection requirements? |  |  |  |
| 93 | Has your organisation ensured that the IWS complies with data protection standards,[[26]](#footnote-27) including through:   * clearly identifying the purpose of the IWS * demonstrating it has assessed and mitigated privacy risks at the IWS design and implementation stages – for example, by performing a data protection impact assessment * applying the principle of data minimisation for the IWS, and only processing personal information that is adequate, relevant and necessary for handling a case * defining proportionate retention periods for the personal information processed in the handling of a whistleblowing report, based on the outcome of the follow-up – for example, for reports found to be beyond the scope of the IWS after an initial assessment, or where an investigation has been launched? * putting into place a personal data protection agreement (DPA) with the service provider, if your organisation has outsourced part of the processing of whistleblowing cases? |  |  |  |
| **Comments and recommendations**: | | | | |

# Support and protection for whistleblowers

Has your organisation considered how to provide protection and support to all categories of potential whistleblowers and protected parties?

| **Questions** | | **Y** | **N** | **P[[27]](#footnote-28)\*** |
| --- | --- | --- | --- | --- |
| Protecting the identity of whistleblowers and other protected persons | | | | |
| 94 | Does the IWS clearly state that without the whistleblower’s explicit consent, their identity and any identifying information should not be disclosed beyond those persons competent to receive or follow up on reports? |  |  |  |
| 95 | Does the IWS specify that where there is a legal obligation to disclose identifying information, the whistleblower must be informed beforehand with sufficient notice, and be provided with a written explanation – for example, that withholding such information would jeopardise related investigations or judicial proceedings–as well as additional protection measures, where appropriate? |  |  |  |
| 96 | Are all persons designated to provide information and handle whistleblower reports bound by a duty of confidentiality, and does your organisation establish penalties for breaching this duty? |  |  |  |
| 97 | Does your organisation take measures to protect the whistleblower and their identity beyond closure of the case? |  |  |  |
| 98 | Does the IWS make clear that anonymous whistleblowers will receive the same level of internal support and protection, should their identity be exposed? |  |  |  |
| **Comments and recommendations**: | | | | |
| Protection from detrimental conduct and interference | | | | |
| Prohibition of detrimental conduct and interference | | | | |
| 99 | Does the IWS clearly prohibit any form of detrimental conduct against whistleblowers and protected third parties – including threats and attempts at detrimental conduct – and establish sanctions for such conduct? |  |  |  |
| 100 | Does the IWS define detrimental conduct broadly, to include any threatened, recommended or actual, direct or indirect act or omission linked to or resulting from actual or suspected whistleblowing, which causes or may cause harm?  In relation to your organisation’s personnel, detrimental conduct includes, but is not limited to:   * suspension, dismissal or equivalent measures * failure to convert a temporary employment contract into a permanent one[[28]](#footnote-29) * early termination of a temporary employment contract, or failure to renew one * constructive discharge, when an organisation makes working conditions intolerable, causing an individual to resign * demotion or withholding of promotion * transfer of duties, reduction or limitation of work assignments, change in working hours * unfair selection for tasks or attendance at events; withholding of training * restrictions on or removal of available resources, such as budgets or human resources * reduction in remuneration or withholding of payment * negative performance assessment or employment reference * unwarranted inspection or investigation of duties, or disclosure of the results of such inspections * imposition or administering of any disciplinary measure, reprimand or other penalty * coercion, intimidation, harassment or ostracism * discrimination, or disadvantageous or unfair treatment * physical or psychological harm or violence * damage to the person’s reputation – for example, smearing, discrediting or humiliating them by questioning their mental health, professional competence, reliability or honesty * financial loss * disclosure of the whistleblower’s identity * prosecution or legal action.   In relation to whistleblowers and protected third parties who are not personnel, detrimental conduct includes, but is not limited to:   * reduction in remuneration or withholding of payment * negative reference * unwarranted audit or evaluation, or disclosure of the results of such audits * coercion, intimidation, harassment or ostracism * discrimination, or disadvantageous or unfair treatment * physical or psychological harm or violence * damage to the person’s reputation – for example, smearing, discrediting or humiliating of a person by questioning their mental health, professional competence, reliability or honesty * financial loss * boycotting or blocklisting * early termination or cancellation of a contract for goods or services * disclosure of the whistleblower’s identity * prosecution or legal action. |  |  |  |
| 101 | Does the IWS clearly prohibit interference or attempts to interfere with whistleblowing, and establish sanctions for such conduct? |  |  |  |
| **Comments and recommendations**: | | | | |
| Preventing detrimental conduct | | | | |
| 102 | Has your organisation expressly committed not to enter into agreements that might waive or obstruct a whistleblower’s rights and protections, including pre-dispute arbitration agreements, loyalty clauses in contracts, or confidentiality or non-disclosure agreements? |  |  |  |
| 103 | Has your organisation included in agreements, contract templates and organisational policies and procedures clauses explicitly recognising the whistleblower rights and protections afforded by its IWS, and stating that in the event of a conflict or perceived conflict with the whistleblowing policy, the whistleblowing policy shall prevail? |  |  |  |
| 104 | Does your organisation ensure that personnel and other stakeholders are made aware that its code of conduct and IWS prohibit detrimental conduct against whistleblowers and other protected persons, and that such conduct will result in sanctions? |  |  |  |
| 105 | Is your organisation implementing strategies to prevent detrimental conduct against whistleblowers throughout the follow-up process and after the conclusion of the case, such as systematic and regular risk assessments and preventive measures? |  |  |  |
| 106 | Does your organisation take measures to prevent risks of further harm to the whistleblower pending the resolution of an internal detrimental conduct complaint – for example, suspending any disciplinary processes against the whistleblower or providing paid leave?[[29]](#footnote-30) |  |  |  |
| 107 | Does your organisation discipline failure to take reasonable steps to prevent detrimental conduct, as a failure of duty by the persons responsible? |  |  |  |
| **Comments and recommendations**: | | | | |
| Addressing detrimental conduct, interference and breaches of confidentiality | | | | |
| 108 | Does the IWS provide enforceable, transparent and timely mechanisms to receive and follow up on complaints about:   * detrimental conduct against whistleblowers and protected third parties * interference or attempts to interfere with whistleblowing * breaches of confidentiality over the whistleblower’s identity? |  |  |  |
| 109 | Once it is established that an individual complaining about detrimental conduct is a whistleblower or another protected person, and that they have suffered detriment, does the IWS require the person accused of the detrimental conduct to clearly and convincingly demonstrate that it was not linked in any way to actual or suspected whistleblowing? |  |  |  |
| 110 | When an individual who complains about detrimental conduct is a whistleblower or another protected person, does your organisation provide them with support measures, such as legal and psychological support, paid leave or retraining? |  |  |  |
| 111 | If the occurrence of detrimental conduct is confirmed, does the IWS state that your organisation shall take necessary action to stop the detrimental conduct and protect the physical, financial and psychological wellbeing of the affected person? |  |  |  |
| 112 | If the occurrence of detrimental conduct is confirmed, does the IWS provide for a full range of restorative actions to remedy the damage caused to the affected person? These include, for example:   * reinstatement of the person either to the position they occupied before detrimental conduct or to a similar position with equal salary, status, duties and working conditions * removal of the person responsible for detrimental conduct, when reinstating the whistleblower or other protected party who put them at risk of further retaliation * fair access to any promotion and training that may have been withheld * restoration of duties, if possible * recognition of lost time and impact on performance * withdrawal of litigation against a whistleblower * deletion of any records that could constitute a dossier for blacklisting or later retaliation * relaunching a procurement process * restoration of a cancelled contract * apologies for failures * commendation for upholding your organisation’s mission, values or interest through speaking up about wrongdoing, through private or, with the whistleblower’s consent, public recognition from senior management – for example, an internal “Speak Up” Award * financial compensation for past, present and future lost earnings * financial compensation for pain and suffering, including medical expenses. |  |  |  |
| **Comments and recommendations**: | | | | |
| Holding the perpetrators of detrimental conduct, interference and breach of confidentiality accountable | | | | |
| 113 | Does your organisation provide for effective, proportionate and dissuasive penalties, following disciplinary proceedings, for:   * detrimental conduct against whistleblowers and protected third parties * interference or attempts to interfere with whistleblowing * breaching confidentiality of the whistleblower’s identity? |  |  |  |
| 114 | Has your organisation established procedures and appropriate penalties to sanction detrimental conduct by persons other than employees, who are not subject to disciplinary procedures, such as consultants, suppliers, persons belonging to the administrative, management or supervisory body, and volunteers? Sanctions could include, for example, removal from a position and termination or non-completion of a contract.   * Are such situations foreseen in your organisation’s contractual arrangements with external parties? |  |  |  |
| **Comments and recommendations**: | | | | |
| Supporting whistleblowers | | | | |
| 115 | When a whistleblower or another protected person complains about detrimental conduct, can your organisation take internal measures to prevent or mitigate harm, such as providing an alternative line manager or workspace, paid leave or retraining? |  |  |  |
| 116 | Does your organisation offer support services to whistleblowers, such as access to psychological support, confidential counselling, legal assistance and peer support networks for whistleblowers, with a focus on those who may face additional challenges due to their social identity – such as gender, race, ethnicity, age, socioeconomic status, sexual orientation or disability? |  |  |  |
| **Comments and recommendations**: | | | | |

# Protection of persons concerned

Does your organisation provide protection measures for the person concerned?

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Questions** | | **Y** | **N** | **P[[30]](#footnote-31)\*** |
| 117 | Does the IWS protect the identity of persons concerned? |  |  |  |
| 118 | Does your organisation protect the rights of persons concerned, including presumption of innocence, the right to respond and the right to receive assistance during the follow-up of a whistleblowing report or a complaint from a whistleblower or a protected third party? |  |  |  |
| 119 | Does the IWS have a process for handling knowingly false reports and warning reporting persons that if they make such a report, they may not be afforded protection under the IWS and may face legal penalties? |  |  |  |
| **Comments and recommendations**: | | | | |

# Continuous monitoring, review and accountability

Does your organisation continuously monitor and regularly review and revise its IWS?

| **Questions** | | **Y** | **N** | **P[[31]](#footnote-32)\*** |
| --- | --- | --- | --- | --- |
| Data collection | | | | |
| 120 | Has your organisation developed indicators to monitor implementation and assess the effectiveness and suitability of the IWS, including:   * the total number of reports received; the number of reports deemed to fall outside the scope of the IWS, and the general reasons why; the number of anonymous reports; the actions taken in response to whistleblowing reports and their outcomes – including the estimated financial damage, compensation, recoveries and sanctions, referral to the authorities, criminal proceedings, the time taken to follow up on reports and the types of wrongdoing reported * the number of complaints of detrimental conduct; actions taken to follow these up, and their outcomes; the time taken to achieve resolution, and types of protection measures taken * feedback from whistleblowers on their experience with the IWS, including recommendations to improve the system * awareness of and trust in the IWS by personnel and other stakeholders it covers – established, for example, by surveys? |  |  |  |
| 121 | Does your organisation have a system to collect the above data, disaggregated in an anonymised form by gender and – where possible – race, ethnicity and disability? |  |  |  |
| **Comments and recommendations**: | | | | |
| Review and amendements | | | | |
| 122 | Does your organisation review the implementation, use, effectiveness and suitability of the IWS, at least annually or more often if needed, based on the above-mentioned indicators and data? |  |  |  |
| 123 | Does your organisation conduct a comprehensive, formal review at least every three years, or more often if needed, of the implementation, use, effectiveness and suitability of the IWS, based on the above-mentioned indicators and data? |  |  |  |
| 124 | Do reviews of the IWS typically answer the following questions:   * One year after the entry into force of the IWS, has your organisation allocated human and financial resources to allow its effective operation? * Has your organisation created a specific department for its ethics or compliance policy and IWS? If not, to which department has it attached the whistleblowing officer or office? * What is the average time taken to provide feedback to a whistleblower? * Has your organisation planned and carried out reviews, internal or external, of the IWS? How regularly? With what results? * Are reviews of the system carried out by the governing body? * Has the IWS been reviewed by a competent authority, such as an anti-corruption agency or whistleblowing authority? If so, with what results? * In the past year, has your organisation:   + - conducted awareness training or other awareness-raising activities regarding the IWS for all potential whistleblowers?     - conducted a survey measuring personnel awareness and trust in the IWS? What were the results?     - received any reports? If so, how many?     - received any complaints of detrimental conduct? If so, how many?     - followed up any reports? If so, how many?     - instigated disciplinary actions or prosecutions as a result of any whistleblowing reports or complaints of detrimental conduct? If so, how many? * Does your organisation have a systematic follow-up procedure to ensure whistleblowers do not suffer reprisals over time – for example, after three months, six months, a year and two years? * Does the whistleblowing officer or office produce an annual report with anonymised data? Who is it shared with and how is it used? * Is the IWS inclusive and gender-sensitive? Does your organisation collect and analyse anonymised, disaggregated data to identify and address reporting patterns and barriers – including detrimental conduct – taking into account gender and other factors that influence individual experiences, such as race, ethnicity or disability? * Does your organisation have a mechanism in place to revise the IWS following audits and annual reports? What is the timeline? |  |  |  |
| 125 | Are there periodic independent reviews of the IWS – for example, by CSOs, a parent company, state authority or professional advisors? |  |  |  |
| 126 | Do reviews involve relevant internal stakeholders, including personnel, personnel representatives, the DEI office or officer, the governing body, and relevant departments and bodies, such as HR, Compliance, Ethics and Legal? Do reviews also include external stakeholders, where relevant, such as subsidiaries, suppliers or CSOs? |  |  |  |
| 127 | Does your organisation revise its IWS according to review findings, to improve effectiveness and ensure systems are up to date and in line with legislation and best practice? |  |  |  |
| **Comments and recommendations**: | | | | |
| Accountability to stakeholders | | | | |
| 128 | Are the above data and review results shared on an annual basis with your organisation’s governing body, personnel and other relevant stakeholders, including shareholders? |  |  |  |
| 129 | Are these annual reports published on your organisation’s website – for example, in the section dedicated to the IWS – and included in relevant reports such as its accountability or governance report? |  |  |  |
| 130 | Are the above data and review results shared in a way that does not reveal any identifying information of the whistleblower and other parties involved, including persons concerned, protected third parties and witnesses? |  |  |  |
| **Comments and recommendations**: | | | | |

# Key principles for internal whistleblowing systems

All public and most private organisations should have an internal whistleblowing system, following these key principles:

## Scope

1. Internal whistleblowing systems should invite reports regarding any suspected wrongdoing – that is, any act or omission that is unlawful, abusive or can cause harm – committed in, by or for the organisation.
2. Internal whistleblowing systems should invite reports from any person who might acquire, in the context of their work-related activities, information on wrongdoing committed in, by or for the organisation.
3. Organisations should protect whistleblowers – that is, any persons reporting suspected wrongdoing with the reasonable belief that the information reported was true at the time of reporting – as well as third parties at risk of detrimental conduct.

## Roles and responsibilities

1. The organisation’s top leadership are responsible and accountable for the effective implementation of its internal whistleblowing system. They should demonstrate their commitment and set a clear “tone from the top” in support of speaking up and listening up about wrongdoing.
2. Organisations should designate an impartial person or department responsible for operation of the internal whistleblowing system. This person or department should be free from conflict of interest, and have sufficient independence, powers and resources, as well as the relevant qualifications.

## Information and communication

1. Information about the organisation’s internal whistleblowing system should be highly visible and accessible, via a wide range of media and channels. All relevant stakeholders, including all potential whistleblowers and persons concerned, should have access to and receive relevant information on the internal whistleblowing system.
2. Organisations should report publicly every year on their commitment to a “speak up and listen up” culture and the implementation of their internal whistleblowing system.

## Procedures

1. Internal whistleblowing systems should include multiple reporting channels that are safe and easily accessible, and enable reporting in writing and orally. Organisations should recognise line managers as possible recipients of whistleblowing reports.
2. Internal whistleblowing systems should ensure diligent follow-up – that is, thorough, timely, fair and impartial – of all reports received,[[32]](#footnote-33) in order to establish whether wrongdoing occurred,[[33]](#footnote-34) to address confirmed wrongdoing and to correct any systemic issue identified.
3. As knowledgeable and interested stakeholders, whistleblowers should be kept informed throughout the process and have meaningful opportunities to provide input to the follow-up of their report.
4. Reports received, follow-up actions, the findings and outcome of the follow-up, and communication with the whistleblower and concerned person should be adequately documented and kept in retrievable and auditable form, in accordance with confidentiality and data-protection requirements.

## Support and protection for whistleblowers

1. Without the explicit consent of the whistleblower, their identity and any identifying information – that is, information from which their identity may be directly or indirectly deduced – should not be disclosed beyond those persons competent to receive or follow up on reports.
2. Organisations should accept and follow up on anonymous reports, and protect anonymous whistleblowers.
3. Organisations should prohibit any form of detrimental conduct – that is, any threatened, recommended or actual act or omission, direct or indirect, which causes or may cause harm – linked to whistleblowing, and any interference with whistleblowing.
4. Organisations should take reasonable steps to prevent detrimental conduct and to ensure that individuals and entities under their control or working for them refrain from detrimental conduct.
5. Internal whistleblowing systems should provide for enforceable, transparent and timely mechanisms to (1) receive and follow up on complaints of detrimental conduct, interference and breach of confidentiality, (2) sanction perpetrators and (3) ensure full reparation to affected whistleblowers and other protected persons, via remedial measures and compensation.
6. Organisations should provide support to whistleblowers to prevent harm to their health or career.

## Protection of person concerned

1. Organisations should protect the identity and the rights of the person concerned, including by providing for effective, proportionate and dissuasive sanctions for individuals who knowingly report false information.

## Continuous monitoring and review

1. Internal whistleblowing systems should be formally reviewed at least annually, and revisions should be made accordingly to improve effectiveness and ensure systems are up to date and in line with legislation and best practice.

Transparency International

International Secretariat

Alt-Moabit 96, 10559 Berlin, Germany

Phone: +49 30 34 38 200

ti@transparency.org

www.transparency.org

Blog: transparency.org/blog  
Facebook: /transparencyinternational  
Twitter/X: @anticorruption  
LinkedIn: @transparency-international  
Instagram: @Transparency\_International   
YouTube: @TransparencyIntl

1. ISO 37002:2021,Whistleblowing management systems — Guidelines. [↑](#footnote-ref-2)
2. ISO 37002:2021,Whistleblowing management systems — Guidelines. [↑](#footnote-ref-3)
3. For example, having an IWS is one of the key metrics of Morgan Stanley Capital International (MSCI) ESG Ratings and the European Sustainability Reporting Standards. [↑](#footnote-ref-4)
4. See, for example, Stephen Stubben and Kyle Welch (2020), Evidence on the Use and Efficacy of Internal Whistleblowing Systems; Bussmann, K-D. & Niemeczek, A. (2019), Compliance through company culture and values: An international study based on the example of corruption prevention. *Journal of Business Ethics*, 157(3), 797–811; Kaptein, M. (2011), From inaction to external whistleblowing: The influence of the ethical culture of organizations on employee responses to observed wrongdoing*, Journal of Business Ethics*, 98, 513–530; Mayer, D.M., Nurmohamed, S., Klebe Treviño, L., Shapiro, D.L. & Schminke, M. (2013), Encouraging Employees to Report Unethical Conduct Internally: It Takes a Village. *Organizational Behavior and Human Decision Processes*, 121, 89-103; Seifert, D.L., Sweeney, J.T., Joireman, J. & Thornton, J.M. (2010). The influence of organizational justice on accountant whistleblowing. *Accounting, Organizations and Society*, 35(7), 707-717. [↑](#footnote-ref-5)
5. Third-party reviewers should acknowledge the inherent limitations of an assessment based solely on publicly available data. [↑](#footnote-ref-6)
6. The EU Directive allows EU member states to exempt municipalities with fewer than 10,000 inhabitants or fewer than 50 workers, and other public entities with fewer than 50 workers, from the obligation to implement an IWS. Therefore, the rule varies among EU countries. [↑](#footnote-ref-7)
7. Even small municipalities routinely take decisions in high-risk areas, such as public procurement, environmental protection and public health, making the presence of IWS critical. The EU Directive allows municipalities to have shared or joint whistleblowing channels, but they still need to implement their own procedures for all other aspects of an IWS. [↑](#footnote-ref-8)
8. Private organisations include organisations from the third sector, i.e. not-for-profit organisations such as civil society organisations, charities and non-governmental organisations. [↑](#footnote-ref-9)
9. This is due to the particular risks of money laundering and terrorist financing. Most private entities providing financial services, products and markets in the EU are required to implement IWS by various EU Directives. [↑](#footnote-ref-10)
10. As smaller entities of the group can easily share resources for the receipt of reports and any investigation to be carried out – for example, through the group-level IWS – the potential administrative and financial burden of implementing an IWS is small and greatly outweighed by its benefits to the organisations and the public interest. [↑](#footnote-ref-11)
11. See the EU Whistleblowing Monitor to follow the progress of transposition of the EU Directive on Whistleblowing across all 27 EU member states, [www.whistleblowingmonitor.eu/](http://www.whistleblowingmonitor.eu/). [↑](#footnote-ref-12)
12. \* Y = Yes; N= No; P = Partially [↑](#footnote-ref-13)
13. \* Y = Yes; N= No; P = Partially [↑](#footnote-ref-14)
14. Some organisations open their IWS to any person who might acquire information on relevant wrongdoing, whether inside or outside the context of their work-related activities, such as users, customers, beneficiaries or local community members. Others implement separate systems to receive and handle reports from “outsiders”. [↑](#footnote-ref-15)
15. \* Y = Yes; N= No; P = Partially [↑](#footnote-ref-16)
16. \* Y = Yes; N= No; P = Partially [↑](#footnote-ref-17)
17. The EU Directive requires IWS to provide clear and easily accessible information regarding the procedures for reporting externally to national competent authorities and, where relevant, to EU institutions, bodies, offices or agencies. [↑](#footnote-ref-18)
18. \* Y = Yes; N= No; P = Partially [↑](#footnote-ref-19)
19. \* Y = Yes; N= No; P = Partially [↑](#footnote-ref-20)
20. The EU Directive requires organisations to establish internal whistleblowing channels that enable reporting in writing or orally, or both. Oral reporting shall be possible by telephone or through other voice messaging systems, and, on request by the reporting person, by means of a physical meeting within a reasonable timeframe. [↑](#footnote-ref-21)
21. The EU Directive requires that internal whistleblowing channels are established and operated in a secure manner that protects the confidentiality of the whistleblower’s identity and of any third party mentioned in the report, and prevents access to that information by non-authorised personnel. [↑](#footnote-ref-22)
22. \* Y = Yes; N= No; P = Partially [↑](#footnote-ref-23)
23. The EU Directive on Whistleblower Protection sets the deadline at seven days. [↑](#footnote-ref-24)
24. The Irish statutory guidance for public bodies and prescribed persons provides good advice on how to assess and monitor risks of detrimental action against whistleblowers and protected third parties. See: Department of Public Expenditure, NDP Delivery and Reform, Protected Disclosures Act – Statutory guidance for public bodies and prescribed persons, November 2023, pp.68-69, <https://www.gov.ie/pdf/?file=https://assets.gov.ie/277081/c8a506a6-1e4c-41de-bc7f-6cba598f7638.pdf#page=null>. [↑](#footnote-ref-25)
25. \* Y = Yes; N= No; P = Partially [↑](#footnote-ref-26)
26. E.g. the EU General Data Protection Regulation (GDPR). [↑](#footnote-ref-27)
27. \* Y = Yes; N= No; P = Partially [↑](#footnote-ref-28)
28. This is in cases where the worker had legitimate expectations that they would be offered permanent employment. [↑](#footnote-ref-29)
29. Once it is established that the individual complaining about detrimental conduct has made an internal or external report, or a public disclosure, and suffered detriment. [↑](#footnote-ref-30)
30. \* Y = Yes; N= No; P = Partially [↑](#footnote-ref-31)
31. \* Y = Yes; N= No; P = Partially [↑](#footnote-ref-32)
32. This includes anonymous reports. [↑](#footnote-ref-33)
33. This also refers to whether wrongdoing is occurring or is like to occur. [↑](#footnote-ref-34)