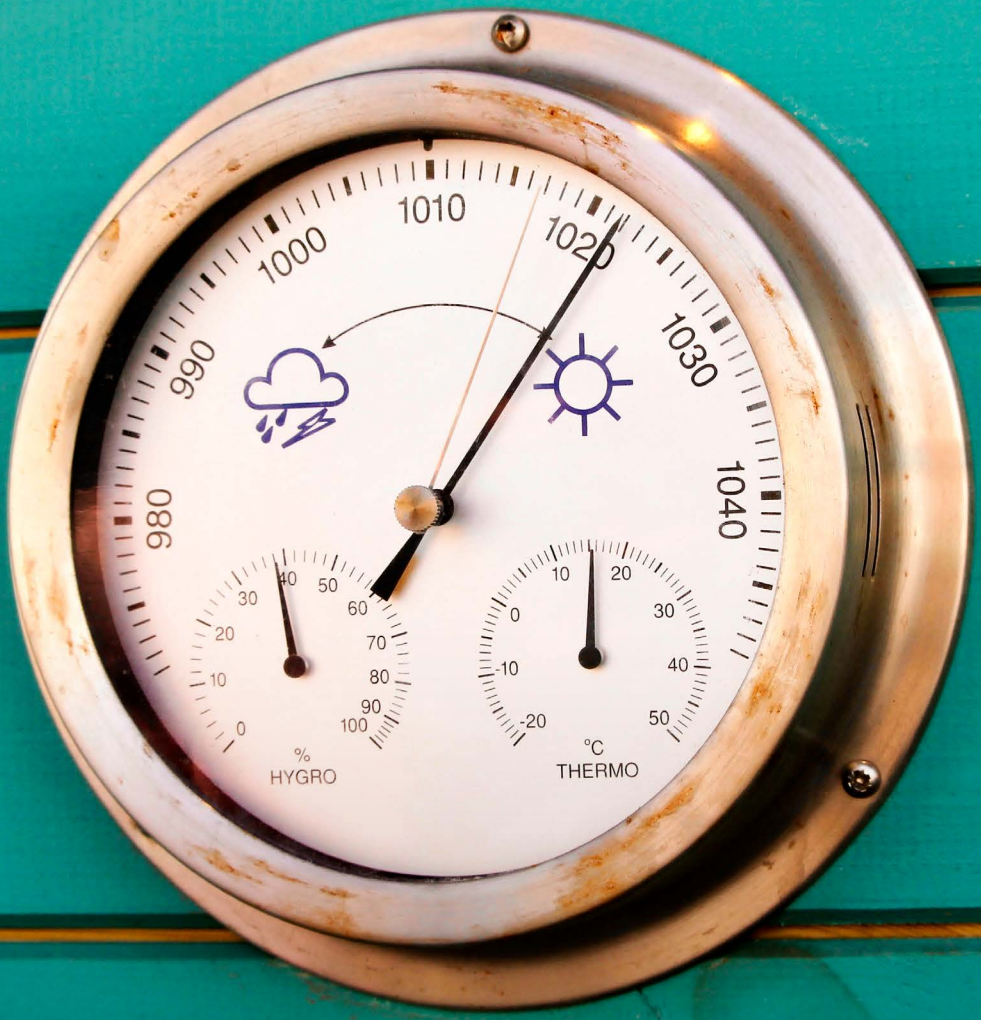
TRANSPARENCY INTERNATIONAL
the global coalition against corruption

TRANSPARENCY INTERNATIONAL IRELAND



MONITORING INTERNAL WHISTLEBLOWING SYSTEMS

A framework for collecting data and reporting on performance and impact

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

Transparency International Ireland is an independent, nonprofit and non-partisan organisation. Its vision is of an Ireland that is open and fair – and where entrusted power is used for the common good. Our mission is to empower people with the support they need to promote integrity and stop corruption in all its forms.

transparency.ie

Monitoring Internal Whistleblowing Systems

A framework for collecting data and reporting on performance and impact

Authors: Ida Nowers and Marie Terracol

Cover: Leon Woods / iStock

Acknowledgements: See page 49

ISBN: 978-3-96076-273-7

Co-funded by the European Union

This publication was produced as part of the "SAFE4Whistleblowers" project, which is co-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.

TABLE OF CONTENTS

GLOSSARY

Whistleblowing report: for the purpose of this guidance, a whistleblowing report is a report that has been assessed by the receiving organisation as falling within the scope of its internal whistleblowing system (IWS).

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

Follow-up: Any action taken to assess, investigate, address and feed back on reports.

Initial assessment: the first step of the follow-up process, to establish factors such as whether the report falls within the scope of the IWS; whether there is a risk of detrimental measures against the reporting person or harm to other parties, the organisation itself or the public interest; whether the report warrants internal investigation, or whether it should be referred to another internal procedure or a reporting or complaint system outside the organisation.

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. For the purpose of this guidance, it includes breach of confidentiality over the identity of a whistleblower and any attempt to hinder whistleblowing.

Whistleblowing officer(s) or office: the person(s) or department designated with responsibility for operation of the IWS.

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

Wrongdoing: any 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 communication of information on suspected wrongdoing made through an organisation's IWS.

External report: a communication of information on suspected wrongdoing made to a designated 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 other than the designated competent authorities (such as journalists, elected officials, civil society organisations, trade unions, or business or professional organisations).

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. These include, for example: persons believed or suspected to be a

whistleblower, even mistakenly; legal entities that the whistleblower owns, works for or is otherwise connected with; third persons connected with the whistleblower, such as colleagues and relatives; persons who assist or attempt to assist a whistleblower.[1]

Personnel: an organisation's employees, officers, directors, agency or temporary workers, trainees and interns.

Personnel representatives: persons recognised as such under national law or practice, e.g. trade union or works council.

Top management: person or group of people who direct and control an organisation at the highest level, i.e. the executives.[2]

Governing body: person or group of people who have ultimate accountability for a whole organisation.[3]

Open reports: a disclosure of information made by a reporting person who voluntarily identifies themselves without requesting confidentiality or anonymity.

Confidential reports: a communication of information made by a reporting person who can be identified by their report, who requests, or is assuming, that their identity will be protected (in line with the IWS provisions, or otherwise on a need-to-know basis).

Anonymous reports: a communication of information made by a reporting person who withholds or attempts to withhold their identity.

Material scope: types of wrongdoing covered by the IWS, i.e. the type of wrongdoing that can be reported and addressed through the IWS, and for which the reporting person will benefit from protection.

Aggregated data: data that has been combined from multiple sources and presented in summary form (e.g. "85 per cent of survey participants in 2025 are aware of the IWS"). It is often used for statistical analysis and insights about a larger population or group, to identify trends, patterns and correlations.

Disaggregated data: data that is broken down into smaller, more specific groups or sub-categories, e.g. male/female/non-binary in case of gender-disaggregated data. It gives an understanding of underlying trends and patterns that might be obscured in aggregated data.

Digital reporting platform: an online system that enables secure, anonymous or confidential reporting and communication with reporting persons.

[1] See Transparency International, *Internal Whistleblowing Systems – Best Practice Principles for public and private organisations*, 2022, p.17.

[2] ISO 37002:2021, *Whistleblowing management systems—Guidelines*.

[3] ISO 37002:2021, *Whistleblowing management systems—Guidelines*.

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 are often themselves best equipped to deal with wrongdoing occurring within their operations, as they have internal knowledge, access to evidence and capacity to respond swiftly. It is also in their interest to make every effort to do so, as it helps minimise liability, reduce financial losses and protect against damage to their reputation. 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, along with robust protection of 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.[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.[5]

Objectives of an IWS

An organisation's IWS has multiple objectives:

- Support and protect personnel and other relevant stakeholders to speak up about wrongdoing.
- Enable early detection and correction of wrongdoing committed within, by or for the organisation.
- Prevent and minimise damage to the organisation, including legal liability, serious financial losses and lasting reputational harm resulting in decreased public trust.

[4] For example, having an IWS is one of the key metrics of Morgan Stanley Capital International ESG Ratings and the European Sustainability Reporting Standards.

[5] 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; 89-103.

- Prevent and minimise damage to the public interest, including public health, human rights and the environment.
- Protect whistleblowers and third parties at risk of detrimental conduct.
- Enable the organisation to learn and remediate.
- Foster an organisational culture of trust, transparency and accountability, which helps prevent wrongdoing.
- Instil trust and confidence in a transparent and accountable public administration.

To achieve its objectives and deliver full benefits, an IWS must be carefully designed and monitored. Organisations should regularly assess the implementation, use, effectiveness and suitability of their IWS – at least annually, or more frequently if necessary – using clear indicators and data. Based on these reviews, they can refine and update their systems to enhance effectiveness and maintain alignment with evolving legislation and best practices.

Additionally, sharing review findings and relevant data annually with governing bodies, personnel and key stakeholders, including shareholders and the public, fosters transparency and accountability. This practice not only strengthens trust in the IWS, but also raises awareness of its role in safeguarding ethical conduct.

OBJECTIVE OF THIS FRAMEWORK

This tool to monitor IWSs includes:

- **A framework of indicators to collect data on the functioning of the IWS**, including on reports of wrongdoing; complaints of detrimental conduct linked to whistleblowing; awareness of and trust in the organisation's IWS, and on the organisation's resources for operation of the IWS.
- **Guidance on collecting and preparing IWS reports**, including key principles, reporting requirements, and roles and responsibilities.
- **Guidance on the IWS report structure and key elements** that should be included to create a comprehensive and impactful IWS report.

Transparency International has developed this guidance and monitoring framework to support:

- organisations across all sectors – public, private and "third" sectors – and jurisdictions, including international organisations, in monitoring, evaluating and reporting on the effectiveness of their IWS, ensuring these are effective and in line with best practice and international standards
- personnel representatives in conducting independent assessments of their organisation's IWS
- compliance professionals assessing other organisations' IWS policymakers and other actors, such as business associations and trade unions, to incorporate data collection and reporting best practices into national and international guidelines on IWS.
- civil society organisations (CSOs) and other actors advocating for effective IWS implementation or developing local or context-specific tools. public administrations in enhancing transparency and ensuring alignment with legal obligations, including to monitor and improve implementation of whistleblowing legislation.

In addition, competent authorities, regulators, ombudspersons, independent whistleblowing authorities and anti-corruption or integrity watchdogs can leverage this monitoring framework to assess the IWS of entities under their oversight or remit. These indicators can help to develop questionnaires to collect data from organisations; aggregate the data collected; identify challenges, best practice and trends, and report their findings to the public. Ultimately, by proposing a common set of indicators to assess the implementation and effectiveness of organisations' IWSs, Transparency International aims to foster a shared understanding across sectors and jurisdictions, helping to identify challenges, promote best practices and improve the protection of whistleblowers, while enhancing the detection and resolution of wrongdoing in organisations, which ultimately safeguards the public interest.

CONTINUOUS MONITORING AND REVIEW

Proper case handling requires organisations to document whistleblowing reports, follow-up actions, findings and outcomes, while ensuring confidentiality and, where necessary, whistleblower anonymity. Many jurisdictions mandate record-keeping for compliance with whistleblowing, anti-corruption, labour or corporate laws. Beyond compliance, systematic documentation strengthens accountability, transparency and ethical governance.

By using a set of indicators to collect, aggregate and analyse whistleblowing data – such as reports received, complaints of retaliation, whistleblower feedback and staff surveys – organisations can identify risks, assess the effectiveness of their IWS and improve protections. To promote inclusivity, anonymised and disaggregated data should be collected by gender and, where possible, by race, ethnicity, disability, sexual orientation, job grade, geographic location and other diversity factors.[6]

Whistleblowing systems must evolve to address emerging risks, internal organisational changes and regulatory developments. Regular audits, trend analysis and independent reviews help refine policies, enhance responsiveness and strengthen protections. A commitment to continuous learning ensures that whistleblowing mechanisms remain effective, fostering a culture of integrity and accountability.

Identifying trends and risks

Tracking whistleblowing cases helps organisations detect patterns of wrongdoing, uncover systemic issues and identify emerging risks. Even where information on suspected wrongdoing is incomplete or inactionable, the intelligence gathered can provide valuable insights to strengthen internal controls and mitigate future risk.

Whistleblowing data can complement existing reporting and provide insights into aspects of organisational performance that are difficult to measure, such as organisational culture and the effectiveness of fraud risk management. In addition, this information helps assess the performance of existing controls and other preventive measures aimed at identifying and deterring misconduct.

Disaggregated data can highlight disparities in how different groups experience wrongdoing, helping address potential biases in workplace culture and response mechanisms.

Evaluating IWS effectiveness

Analysing case and other data allows organisations to assess whether their IWS is accessible, trusted and effective in addressing misconduct.

For instance:

- A low number of reports may indicate a need for awareness raising, particularly among underrepresented groups.
- A high proportion of reports falling outside the IWS's scope may highlight the need for staff training on reporting mechanisms.
- Staff surveys can provide insights into trust levels in the IWS across demographic groups.

Regular IWS reviews help refine policies to align with legal requirements, best practices and inclusivity standards.

Assessing protection measures

Monitoring complaints of retaliation helps assess whether whistleblowers may face adverse consequences, and whether complaints are likely to lead to meaningful corrective actions. Disaggregated data analysis can reveal whether certain groups are more vulnerable to retaliation, or if specific cases receive unequal attention or resolution.

TRANSPARENCY AND ACCOUNTABILITY TO STAKEHOLDERS

Comprehensive reporting on the use and effectiveness of an organisation's IWS has several benefits for both public and private organisations, as well as competent authorities. Publishing a high-quality IWS report for both personnel and the public ensures accountability, improves organisational compliance, and builds and signals a safer environment for whistleblowers.

[6] See the section on key principles guiding data recording and reporting for best practices to aggregate data to safeguard whistleblower identities.

Building trust and confidence

Publishing data on whistleblowing reports builds confidence among personnel, governance bodies, customers, insurers, shareholders and investors, regulators and the wider public. It demonstrates that the organisation takes concerns seriously, protects whistleblowers, and is committed to accountability and ethical conduct.

Transparent reporting also strengthens trust in the IWS itself, reinforcing its role as a reliable effective mechanism for addressing wrongdoing. It signals that an organisation fosters a culture which prioritises the highest ethical standards.

Internally, robust data reporting also enables the development of meaningful metrics that can be integrated into existing management routines. This gives top leadership and governing bodies greater confidence that the IWS and broader wrongdoing prevention efforts are being proactively managed, and are more than an incident to respond to or a topic to discuss.

Feedback

Regular reporting to staff on themes and trends on the outcomes and impact of reports serves as a vital feedback mechanism, particularly in cases where confidentiality or legal constraints limit direct updates on follow-up actions to individual reporting persons. Feedback is essential to an effective IWS, to overcome fear of futility, which is the predominant reason people do not speak up. While an IWS report may not be able to provide case-specific details, it helps demonstrate that concerns raised through the IWS contribute to broader improvements and accountability. Case outcomes, such as the number of disciplinary actions taken, can also demonstrate an organisation's zero-tolerance policy to wrongdoing, without breaching the privacy and employment rights of those involved.

Equally important is gathering and reporting feedback from whistleblowers who have used the IWS. Their insights help organisations understand how the IWS works in practice and identify gaps, to improve procedures and strengthen the "speak up culture". The IWS report itself presents an opportunity to demonstrate that the organisation actively seeks such perspectives and is genuinely committed to meaningful engagement and continuous improvement.

By demonstrating that reports lead to meaningful change, organisations encourage future reporting and reinforce a "speak up, listen up culture".

COLLECTING DATA AND PREPARING THE REPORT

KEY PRINCIPLES GUIDING DATA COLLECTION AND REPORTING

The following key principles should guide the reporting process to ensure that the IWS remains transparent, accessible and aligned with best practices.

Confidentiality: protecting identities and ensuring safety

Confidentiality is the cornerstone of effective whistleblowing systems. Both data collection and reporting must be designed and structured to safeguard the identities of whistleblowers, as well as persons concerned, protected third parties and witnesses. To prevent potential identification and retaliation, organisations must implement robust security measures at every stage of the process. This includes:

- **Need-to-know access**: Only those who are trained and with a direct and essential role in handling whistleblowing data should have access. Any identifying information on whistleblowers should be protected with controlled access logs, to monitor any attempts to retrieve sensitive information.
- **Secure systems**: Sensitive information and data must be stored and transferred using segregated systems which utilise best-practice encryption, password protection and multi-factor authentication to prevent unauthorised use.

Best practices for confidentiality in reporting

Before including any information in the report, organisations should conduct rigorous risk assessments to evaluate and prevent identification and retaliation. Key considerations include:

- **Assessing indirect identification risks**: Even without providing names or job details, whistleblowing reports and case studies may inadvertently reveal a whistleblower's identity, particularly in small organisations or cases with unique circumstances.
- **Obtaining informed consent**: If identifiable information is necessary and proportionate for reporting aims, explicit consent must be obtained from the whistleblower.

To further minimise identification risks in the IWS report, organisations should consider:

- **Using data aggregation**: Instead of disclosing exact case numbers, organisations could report data in broader ranges or categories, e.g. "none", "1-3" or "1-5". Exact figures could be given only when the number is greater than three or five, to minimise the risk of unintentionally exposing individuals when the organisation is

small or there are a low number of cases.

- **Redacting or generalising case details**: Organisations should consider pseudonymising or generalising details, to prevent patterns from revealing identities.
- **Utilising secure digital reporting technology**: Organisations should implement secure digital reporting platforms that enable safe submission, storage and management of reports and related data, as well as two-way communication with anonymous reporting persons. Platforms such as GlobaLeaks offer free, open-source, encrypted software.

Data integrity

To ensure that the data collected reflects the true performance of the IWS, organisations should maintain high standards of data integrity. This requires that all data related to whistleblowing is collected, stored and reported in a way that is accurate, complete, consistent and reliable. This necessitates the establishment of robust data collection processes, including clear timelines, standardised definitions and categories when collecting whistleblowing data, as well as safeguards against unauthorised changes, bias and selective reporting.

This builds confidence in the integrity of the system and ensures that reported metrics reflect the true performance of the IWS.

Accessibility: making IWS data clear and easy to find

To be effective, whistleblowing data must be both accessible and understandable to all relevant stakeholders, including employees, regulatory bodies and, where appropriate, the public. Data collection methods should be designed to capture relevant information in a structured and meaningful way, while reports should be clear, easy to understand, and available in multiple formats and local languages, if needed.

In the spirit of "continuous communication", organisations should publish whistleblowing data in a dedicated section of their website, and integrate key findings into broader reports, such as accountability or governance reports, ensuring that stakeholders can readily access and interpret the information.

Gender equality and social inclusion: ensuring inclusive systems

Data collection should be designed to identify and address disparities in whistleblowing engagement. Gender-disaggregated data, along with other relevant demographic indicators – such as age, ethnicity, sexual orientation, neurodiversity, disability, job grade, geographic location and other diversity factors – can highlight potential biases or barriers within the system, helping to ensure fair and equal protection for all.

Beyond whistleblower engagement, analysing this data can reveal broader organisational trends, such as whether certain types of wrongdoing disproportionately affect women or other specific groups, and whether there are differences in detrimental conduct faced by whistleblowers of different demographics. Understanding these patterns allows organisations to take targeted action to address systemic issues and strengthen protections.

By collecting and reporting this data, organisations reinforce their commitment to inclusivity, fairness and accountability, demonstrating that their whistleblowing systems are accessible and protective to all individuals, regardless of gender, background or status.

Caution: When collecting and reporting disaggregated demographic data, organisations must take care to ensure that the whistleblower's identity is not inadvertently exposed. The need for confidentiality and protection should always take priority, to avoid compromising safety and undermining trust in the IWS.

UNDERSTANDING REPORTING REQUIREMENTS

When preparing an IWS report, it is essential to ensure compliance with legal obligations, adherence to industry standards, and alignment with best-practice principles.

Legal compliance

To meet their reporting obligations, organisations must carefully review all relevant laws and

regulations, in particular those governing the collection, aggregation and reporting of whistleblowing-related data. This review should begin with any applicable whistleblower protection legislation, and extend to related legal frameworks, including data protection laws, corporate governance codes and public oversight mechanisms. Additionally, organisations must consider broader regulatory requirements that may intersect with whistleblowing, such as those addressing anti-corruption, anti-money laundering, anti-bribery or labour practices.

For organisations operating in regulated sectors such as health care, finance or public services, additional sector-specific requirements may apply. Multinational entities must also navigate extra-territorial regulations to ensure compliance across all jurisdictions in which they operate.

Organisations' commitment to standards

Many organisations voluntarily adhere to best-practice standards for IWS. These include those from the International Organization for Standardization, such as ISO 37002 for internal whistleblowing systems and ISO 37001 for anti-bribery management, as well as industry-specific benchmarks. Organisations should assess the data collection and reporting requirements outlined in these standards, to ensure alignment. Additionally, ESG reporting frameworks, such as the Global Reporting Initiative and the Sustainability Accounting Standards Board, increasingly emphasise whistleblowing and corporate ethics as key indicators of governance and organisational integrity.

Best-practice principles

Beyond legal compliance and internal standards, organisations should ensure that the collection, aggregation and reporting of whistleblowing data align with internationally recognised best practices. Guidance from Transparency International, such as this, and from other global organisations provides frameworks for systematically gathering and analysing whistleblowing data to enhance transparency, improve whistleblower protection and strengthen case management.

By adhering to these best practices, organisations can ensure consistency in data collection methods, maintain accurate records of reports and outcomes, and produce reliable, insightful reporting. Integrating these principles into whistleblowing data management not only reinforces internal accountability, but also demonstrates a proactive commitment to ethical governance reporting standards.

Record keeping and data protection

Ensuring a robust and compliant IWS requires careful documentation and strict adherence to general data protection standards. Organisations must comply with all national and other applicable regulations, such as the European General Data Protection Regulation, to ensure privacy and security. Organisations must record reports received, follow-up actions, findings and outcomes. Such records should be securely stored for a proportionate period – long enough to allow for thorough follow-up, protect whistleblowers from retaliation, and uphold the rights of those implicated, but never longer than necessary.

To maintain integrity and transparency, records must be kept in a retrievable and auditable format, while complying with confidentiality and data protection regulations. Organisations should ensure their IWS aligns with data protection standards by clearly defining its purpose, assessing and mitigating privacy risks at both design and implementation stages – such as through a data protection impact assessment – and applying the principle of data minimisation, ensuring only relevant and necessary personal information is processed.

Retention periods for personal data should be proportionate to the follow-up process, with specific guidelines for cases deemed outside the scope of the IWS or those leading to an investigation. If whistleblowing case processing is outsourced, organisations must also establish a personal data protection agreement with service providers, to safeguard sensitive information. By implementing these measures, organisations can ensure their whistleblowing processes remain secure, compliant and effective in fostering trust and accountability.

ROLES AND RESPONSIBILITIES IN DATA COLLECTING AND REPORTING

The organisation's top leadership – its senior management and governing body – holds ultimate responsibility for the effective implementation of the IWS. As part of their oversight duties, the governing body, the head of the organisation and, in the case of multinational companies, the head office or regional offices should receive regular reports on the IWS's operation, to evaluate its effectiveness and ensure it remains fit for purpose.

The whistleblowing officer or office responsible for managing the IWS is also responsible for monitoring, reviewing and reporting on its implementation. This includes providing regular updates to top management and the governing body. Additionally, they are responsible for preparing reports to other key stakeholders, such as regulators, shareholders, employees and the public, on the usage, outcomes and lessons learned from the whistleblowing system.

To compile these reports, the whistleblowing officer may need to collect data from various functions, including Human Resources, Finance and Internal Audit, as well as from different internal reporting and complaint mechanisms. In many organisations, complaints related to detrimental conduct fall outside the scope of the IWS and are handled by separate internal complaints systems, such as grievance mechanisms. Therefore, the department or individual responsible for handling such complaints and maintaining related records may not always be the whistleblowing officer or office. Clear coordination and data-sharing processes are essential to ensure accurate and comprehensive reporting.

UNDERSTANDING THE REPORT'S AUDIENCE

When preparing an IWS report, it is important to tailor the content to suit different stakeholders. The level of detail, tone and focus may need to be adapted based on whether the report is for an internal or external audience. In some cases, separate reports may be required for different groups.

Governing body and top management

The report for the governing body and top management should focus on high-level insights driven by the analysis of aggregated data collected, emphasising key trends, risks and areas for improvement. The whistleblowing officer or office should ensure the report is strategic, solution-oriented and aligned with governance priorities. Key areas to highlight include:

- **IWS effectiveness risks**: complaints about detrimental treatment, delays in meeting timeframes, capacity issues and missed whistleblowing cases.
- **Trust and confidence issues**: poor outcomes from staff surveys, exit interviews or negative feedback from whistleblowers who have used the IWS.
- **Reputational and legal risks**: negative media coverage, litigation and action points to improve the IWS, such as policy reviews.

Governing bodies should take a proactive approach in reviewing reports on the organisation's IWS, holding themselves accountable for any system failures and driving continuous improvement.

The organisation's personnel

For personnel, the IWS report should serve as an opportunity to raise awareness of the IWS. It should reiterate the whistleblowing process, key assurances and personnel involved, and signpost any available support and protections. It should highlight positive outcomes, success stories and testimonials, to build trust and confidence.

When using case studies to illustrate effective outcomes, organisations must be particularly mindful to ensure confidentiality is maintained, as tiny fragments of identifying information can be pieced together by personnel, especially in smaller organisations, given their internal knowledge.

The report is an opportunity for the top leadership to demonstrate to staff groups its commitment to the IWS, and to endorse key findings to reinforce the "tone from the top". Where failures have been identified, they should be acknowledged openly. Transparency about mistakes helps build confidence and reassures staff that commitments to improvements are genuine.

When communicating with personnel groups, the organisation should focus on being clear, reassuring and transparent, emphasising the importance of safeguards in place to protect them, and the

availability of independent advice or employee assistance programmes.

External stakeholders

A published IWS report should be structured to communicate effectively with a wide audience. A diverse range of stakeholders may take interest in the findings, including regulators, independent whistleblowing authorities, policymakers, trade unions, CSOs and even parliamentary committees, as well as the organisation's contractors and volunteers.

Shareholders and investors are also increasingly recognising the importance of IWSs as an essential component of risk management, and may therefore request IWS data and reports as part of their engagement with investee companies.[7]

Additionally, organisations should also consider the broader public, potential customers, clients, beneficiaries, funders and service users, as well as potential whistleblowers, when compiling an IWS report.

PUBLICATION AND PROMOTION

Information about the organisation's IWS should be highly visible and easily accessible through a variety of media and communication channels. All relevant stakeholders must have access to clear and comprehensive information about the IWS. This includes reports on its operation, as well as efforts to foster a "speak up and listen up" culture. Ensuring transparency in this way builds trust and encourages engagement with the system.

Organisations should post their public annual IWS report on their website, ideally within a dedicated IWS section, and share such reports through their usual communication channels, including social media. The data and findings should also be included in broader reports, such as annual accountability or governance reports, although this should not replace a standalone publication.

Internally, annual and periodic reports, such as quarterly or semi-annual updates, should be made readily accessible to employees and key stakeholders – for example, through the organisation's intranet – and proactively shared via email, internal newsletters, workplace social networks and presentations at general staff meetings.

Where applicable, reports should be made available in multiple languages and accessible formats, to ensure inclusivity.

[7] See Principles for Responsible Investment (2020), Whistleblowing: Why and how to engage with investee companies, https://www.unpri.org/sustainability-issues/environmental-social-and-governance-issues/governance-issues/whistleblowing.

THE IWS REPORT

A well-structured IWS report is essential for clearly communicating the performance of an organisation's IWS, ensuring transparency and accountability. This section provides guidance on the key elements that should be included to create a comprehensive and impactful report.

PART I – ESTABLISHING THE FRAMEWORK

Overview of whistleblowing requirements

To establish a clear foundation, the report should outline the current legal and regulatory requirements governing whistleblowing within the organisation, with a particular emphasis on data collection and reporting obligations. Clearly defining these commitments and requirements underscores the organisation's dedication to compliance with evolving regulation and best practices, as well as protecting whistleblowers and addressing misconduct.

In addition, the report should provide an overview of the IWS, detailing its scope and the protection it offers. This section should also highlight any recent reforms or changes to policies, procedures or key individuals taking part in the IWS operation that have strengthened or weakened the system. This could include updates to safeguarding mechanisms for whistleblowers.

Capacity and resource allocation

For an IWS to function effectively, adequate financial, human and technological resources must be allocated. This section of the IWS report should provide an overview of the organisation's investment in its IWS. This includes:

- human resources: number of relevant personnel and their training, and any external consultants
- financial resources: the annual budget and actual expenditure on the IWS
- an overview of the system's technological infrastructure.

Where relevant, the report should highlight any changes in resource allocation – such as increased funding, underfunding concerns or anticipated adjustments – to demonstrate organisational commitment to effective whistleblowing or to identify potential challenges.

PART II – THE VALUE OF WHISTLEBLOWING

Whistleblowing is a crucial tool for upholding ethical standards, preventing harm and maintaining public trust. This section should emphasise its importance, both for the organisation and the wider public interest.

Encouraging employees and stakeholders to report concerns requires fostering a culture where the importance of whistleblowing is understood, and sharing information and concerns is supported. The report should reiterate the importance of whistleblowing generally, as well as to the organisation concerned. It should also explain what whistleblowing entails, reiterate the protections available to all whistleblowers and outline any support measures for them.

Tone from the top

Leadership statements on the importance of whistleblowers and how they are positively regarded by the organisation should reinforce a "tone from the top" demonstrating commitment to an effective and inclusive IWS, as well as transparency and ethical governance.

PART III – DATA ON REPORTS

This section of an organisation's report should present a detailed analysis of the data collected from its IWS. The monitoring framework for evaluation of the IWS is outlined on page 19 of this guidance. The content and focus of the report will be tailored to its intended audience (see "Understanding your report's audience" on page 14 for further details). For example, separate reports may be prepared for different stakeholders, such as a quarterly update for the governing body, and an annual public report published on the organisation's website.

Statement on confidentiality

Ensuring the confidentiality of whistleblowers and persons concerned is paramount. The report should include a statement affirming that all data has been reviewed to mitigate the risk of identification of whistleblowers or other individuals involved. Best practices include avoiding the publication of low numbers of whistleblowing reports, to prevent inadvertent identification, instead using ranges such as "zero", "1-3", or "four and above".

The statement should be followed by a reassurance that the organisation takes a zero-tolerance approach to detrimental conduct against whistleblowers.

Clarifying data scope

Transparency in reporting requires clear definitions of data scope and methodology. The report should specify the reporting period and publication schedule, as well as any third-party platforms or independent advisors used to manage reports. This ensures clarity on how data is handled, stored and protected.

Presenting the data

Presenting the data in a structured way is essential for assessing trends and system performance. This section of the IWS report should present key indicators, highlight trends compared to previous periods, and identify any emerging risks.

Including gender-disaggregated data allows organisations to analyse potential disparities in reporting patterns. Where relevant, narrative insights should explain whether certain groups face barriers in raising concerns, ensuring that whistleblowing systems remain accessible to all.

Key information to be reported: best-practice recommendation

The organisation's reporting should cover information on the use, outcomes and lessons learned from the IWS. This will include both anonymised aggregated and disaggregated data on the receipts and handling of reports of wrongdoing, complaints of retaliation, awareness and trust in the IWS, and resources (see the monitoring framework).

Data on reports of wrongdoing

This should include:

- the total number of reports received, and channels used
- the number of anonymous reports
- the number of reports deemed to fall outside the scope of the IWS, and the main reasons why
- the actions taken in response to whistleblowing reports and their outcomes – including the estimated financial damage; the value of the harm prevented; compensation; asset recoveries; disciplinary sanctions; referral to the authorities; civil, administrative or criminal proceedings, and changes in policy or procedure
- the time taken to follow up on reports
- the types of wrongdoing reported
- the type of reporting person
- whistleblowers' satisfaction rate on their experience with the IWS

- changes to the IWS policies, procedures or processes, following feedback from whistleblowers.

Data on the organisation's protection of whistleblowers

This should include:

- the number of complaints of detrimental conduct received
- the outcome status of the complaints (whether substantiated or not)
- the type of detrimental treatment uncovered
- actions taken to follow up on these complaints, and their outcomes
- the time taken to achieve resolution
- the number of instances where protection or corrective measures were applied
- the types of protection measures taken to prevent or address detrimental conduct
- whistleblowers' satisfaction rate on their experience with the complaint mechanism
- changes to the complaint mechanism policies, procedures or processes, following feedback from whistleblowers.

Data on awareness of and trust in the organisation's IWS

This should include:

- percentage of staff and managers trained
- percentage of staff who know how to report wrongdoing (obtained via personnel survey)
- percentage of staff who trust the IWS.

Case examples and outcomes

Anonymised case studies illustrate the types of concerns reported and the actions taken. Presenting these in a "you said, we did" format can enhance engagement and showcase the organisation's responsiveness. Care should be taken to protect confidentiality and avoid revealing identifying details.

Feedback and continuous improvement

Whistleblower feedback is vital for refining the IWS. This section of the report should present insights from whistleblowers on their reporting experience and any changes implemented to enhance the system.

PART IV – THE IMPACT OF WHISTLEBLOWING ON THE ORGANISATION

The final section should assess how whistleblowing contributes to the organisation's mission, remit, strategic goals and ethics. Whistleblowing reports often serve as an early warning system, helping to identify risks, strengthen governance and improve compliance.

The IWS report should demonstrate the tangible impact of whistleblowing by showcasing policy updates, procedural improvements or cultural shifts that have resulted from whistleblower reports. Where applicable, it should provide examples of how whistleblowing has led to enhanced risk management, cost savings, prevention or mitigation of harms to the organisation or the general public, or regulatory changes.

Illustrating the impact of whistleblowing through case studies can further emphasise its value. Examples may include cases where reporting led to positive outcomes, as well as situations where failure to report resulted in harm – such as threats to consumer protection or public health. Tailoring these examples to the organisation's sector can help strengthen relevance and engagement.

Ultimately, this section should emphasise how addressing reported concerns strengthens the organisation's ability to fulfil its objectives, protect its reputation and maintain public trust. Linking whistleblowing to core values and long-term sustainability ensures that employees and stakeholders recognise its importance in upholding integrity and accountability.

MONITORING FRAMEWORK

This monitoring framework provides indicators to collect data on reports of wrongdoing; complaints of detrimental conduct linked to whistleblowing awareness and trust in the organisation's IWS, and the organisation's resources for operation of its IWS. It is mainly intended for data collection purposes and does not imply that all the data collected should be included in the IWS report(s). In certain cases, reporting such data could risk exposing the identifying information of a whistleblower. Guidelines on what should be included in the IWS report are outlined in the sections "Collecting data and preparing the report" and "The IWS report".

INDICATORS ON REPORTS OF WRONGDOING

This section includes two sets of indicators. The first concerns all the reports received through the IWS channels. The second focuses on the reports that were assessed by the organisation as being whistleblowing reports.

Indicators on all reports of wrongdoing received through the IWS

This set of indicators concerns all the reports received through the organisation's IWS channels.

Indicator #	Indicators on reports received	Disaggregated by gender	Guidance
1	**# of reports received**	Yes	Repeated reports by the same person on the same wrongdoing should be counted as one report.
2	**Reporting channel used:** Breakdown of # of reports received per **reporting channel**, for example: • digital platform • email • physical meetings • post • on-site "letter boxes"	Yes	

Indicator #	Indicators on reports received	Disaggregated by gender	Guidance
	• telephone • external hotline provider • transfer from another internal complaint system • transfer from line managers • transfer from members of the governing body and top management.		
3	**Type of reporting person:** Breakdown of # of reports received, by type of reporting person, for example: • personnel (excluding volunteers and paid or unpaid trainees) • volunteers and paid or unpaid trainees • self-employed persons • shareholders and persons belonging to the administrative, management or supervisory body • 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 • others.	Yes	**Record** whether the reporting person was still in that position when making their report, or had already left that position.
4	**Confidential, anonymous or open:** Breakdown of # of reports received, based on whether and how the reporting person chose to share their identity: • confidential report • anonymous report • open report.	Yes	The percentage of anonymous vs non-anonymous reports may be an indication of trust over time. A pattern of decreasing anonymous reporting and increasing non-anonymous reporting could indicate trust building up, and potentially improvement in the "speak up" culture of the organisation.
5	**Reports initially assessed:** # of reports received that have gone through an initial assessment, including overflow from previous periods.		

Indicator #	Indicators on reports received	Disaggregated by gender	Guidance
6	**Outcome of the initial assessment:** Breakdown of # of reports received, by outcome of the initial assessment: • reports found to fall outside the scope of the organisation's IWS • reports found to fall inside the scope of the organisation's IWS.		
7	**Reasons reports fell outside the IWS scope:** Breakdown of # of reports found to fall outside the IWS scope following initial assessment, by main reasons, including: • the reporting person does not have a work-based relationship with the organisation • the type of wrongdoing reported falls outside the material scope of the IWS • the wrongdoing reported does not have any direct or indirect link with the organisation.		**Record** the type of wrongdoing reported that falls outside the scope of the IWS. Trends might provide useful information to improve the IWS and other internal reporting and complaint systems.
8	**Closure actions for out-of-scope reports:** Breakdown of # of out-of-scope reports, by actions taken to close them, including: • referral to another internal procedure, such as other internal reporting or complaint system • referral to a reporting or complaint system outside the organisation • #closure with no further action.		**Record** which internal reporting or complaint system the report or reporting person was referred to, and why. Trends might provide useful information to improve the IWS and its articulation with other internal reporting and complaint systems. **Record** to which external reporting or complaint system the report or reporting person was referred to, and why.
9	**Appeals of initial assessment outcome:** Percentage of reports where the initial assessment outcome was appealed.	Yes	**Record** reasons for the appeal and outcome.
10	**Retaliation risks:** Percentage of reporting persons assessed to be at risk of detrimental conduct.	Yes	
11	**Acknowledgement of receipt:** Percentage of reports with acknowledgement of receipt within target period.		The target period is the timeframe pre-established by the organisation to acknowledge receipt of reports.

Indicator #	Indicators on reports received	Disaggregated by gender	Guidance
12	**Initial assessment duration:** Average time to conduct initial assessment of reports.		Collecting this data helps assess the effectiveness of the IWS. Publishing this data helps inform potential whistleblowers about what to expect when reporting.

Indicators on whistleblowing reports received

This set of indicators focuses on reports received that have been found to fall inside the IWS scope following initial assessment, i.e. the "whistleblowing reports" as defined in the organisation's IWS.

Indicator #	Indicator	Disaggregated by gender	Guidance
13	**# of whistleblowing reports (i.e. reports found to be falling within the scope of the IWS) followed up during the year, including overflow from previous years.**	Yes	
14	**Reports within scope of whistleblowing law:** # of whistleblowing reports falling within the scope of the national whistleblower protection law.	Yes	This data should be collected if the scope of the organisation's IWS is wider than the scope of the law.
15	**Time of receipt of whistleblowing reports with follow-up during the year:** Breakdown of # of whistleblowing reports (as defined by the organisation's IWS[8]) followed up during the year, by year of receipt of the report: • reports received during the year • reports received the year before • reports received prior to the year before.	Yes	

[8] All following indicators concern whistleblowing reports as defined by the organisation's IWS. The legal definition might be narrower.

Indicator #	Indicator	Disaggregated by gender	Guidance
16	**Confidential, anonymous or open:** Breakdown of # of whistleblowing reports followed up during the year, based on whether and how the whistleblower chose to share their identity: • confidential report • anonymous report • open report.		The percentage of anonymous vs non-anonymous reports may be an indication of trust over time. A pattern of decreasing anonymous reporting and increasing non-anonymous reporting, could indicate trust building up, and potentially improvement in the "speak up" culture of the organisation.
17	**Identification of anonymous whistleblowers:** Breakdown of # of reports where an anonymous whistleblower was identified, by reason for the identification (as a percentage): • voluntary disclosure of identity by the whistleblower to a person involved in handling the report • voluntary or inadvertent breach of confidentiality by a person involved in handling the report • other, e.g. circumstances of the case.	Yes	The first is an indicator of trust in the IWS. The second indicates need for a review of its effectiveness in protecting the identity of the reporting person.
18	**Disclosure of whistleblower's identity:** # of confidential reports that required disclosure of the whistleblower's identity.		Record the justification for such disclosure.
19	**Reopened whistleblowing reports:** # of whistleblowing reports reopened during the year due to new information warranting renewed follow-up, and breakdown by outcomes: • founded • unfounded.	Yes	
20	**Status of whistleblowing reports:** Breakdown of # of whistleblowing reports with follow-up during the year, by status of report at the end of the year: • reports closed • reports with ongoing follow-up.		

Indicator #	Indicator	Disaggregated by gender	Guidance
21	**Whistleblowing report initial assessment outcomes:** Breakdown of # of whistleblowing reports assessed during the year, by outcome of the assessment: • initiation of internal investigation • referral to another internal procedure, such as other internal reporting or complaint system • referral to a reporting or complaint system outside the organisation • closure with no further action • assessment still ongoing at year-end.	Yes	**Record:** • which internal reporting or complaint system and which external authorities the report or reporting person was referred to, where relevant, and outcomes, if known • the reasons why a report was closed at the initial assessment stage with no further action, e.g. lack of evidence.
22	**Protection measures:** • # of reports where measures to prevent or mitigate risks of detrimental conduct against the whistleblower were taken • # of reports where measures to prevent or mitigate risks of harm to other parties, the organisation itself or the public interest were taken • # of reports where other protection measures were taken.		**Record** the types of preventative or mitigation measures taken and the circumstances that called for them. **Note:** A single report may result in multiple measures and should be counted in each relevant category.
23	**Follow-up outcomes:** Breakdown of # of whistleblowing reports closed during the year, by outcomes of the follow-up: • no wrongdoing was found • insufficient evidence to confirm wrongdoing • wrongdoing found to have occurred • imminent risk of actual wrongdoing identified.	Yes	
24	**Types of wrongdoing identified:** Breakdown of # of whistleblowing reports where wrongdoing was found to have occurred or where imminent risk of actual wrongdoing was identified, by type of wrongdoing, for example: • criminal offences • breaches of legal obligations (national and international) • dangers to the public and occupational health and safety	Yes	When deciding the categories of wrongdoing into which the data should be broken down, organisations should take into consideration the types of wrongdoings covered by national law, and the types of wrongdoing covered by the organisation's code of conduct.

Indicator #	Indicator	Disaggregated by gender	Guidance
	• dangers to the environment • human rights violations • child exploitation or abuse • gender-based violence, harassment, bullying and discrimination • corruption[9] • 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 the organisation[10] • attempted or actual concealment of wrongdoing, including interfering or attempting to interfere with whistleblowing.		
25	**Remedial actions:** # of each type of action taken by the organisation to address wrongdoing found to have occurred or imminent risks of actual wrongdoing identified, for example: • referral to external authorities, such as regulators (including self-reporting) • initiation of disciplinary proceedings • instigation of civil or administrative lawsuits • lodging of a criminal complaint		**Record**: • name of external authorities involved and the outcome (if known) • the outcomes of disciplinary proceedings (e.g. sanctions issued) • status and outcomes of any civil, administrative and criminal proceedings

[9] This includes bribery, money laundering, sexual corruption, embezzlement, misappropriation, abuse of authority, obstruction of justice and illicit enrichment.

[10] Because such conduct is harmful to its interests, reputation, operations, financial wellbeing or governance, or violates in any other way the organisation's codes of conduct or ethics, and relevant policies.

Indicator #	Indicator	Disaggregated by gender	Guidance
	• internal measures to recover assets • voluntary financial and other settlements to remedy the wrongdoing and the costs of preventing impending harm • interim measures, e.g. suspension from post, to prevent or mitigate wrongdoing, risks or impending harm to persons, the organisation itself or the public interest.		• the total amount of assets recovered internally or via external proceedings, and the method of recovery, e.g. restitution, seizure, if known • the type and amount of any voluntary remedy (e.g. financial compensation, service reinstatement) and value (and any rationale or aim, if known). **Note:** A single report may result in multiple actions and should be counted in each relevant category.
26	**Systemic corrective actions:** # of whistleblowing reports where actions were taken to correct a systemic issue identified, such as weaknesses in policy, procedure or controls, whether or not the investigation revealed wrongdoing.		**Record**: the weaknesses identified and action taken to address them.
27	**Financial impact of remedial actions:** Actual and estimated financial impacts of measures taken as a result of follow-up on a report, including recovered expenditures, damages awarded, financial recoveries, or other loss or waste reduction.		**Record**: both actual and estimated: • financial recoveries • damages awarded • reduced expenditures, e.g. lower legal fees; fines or penalties avoided • loss or waste reduction • monetary benefits (savings) to the public purse as a result of risks identified or mitigated through IWS reports • improved resource use or prevention of misuse or abuse of public funds. Record both the total amount during the reporting period and the running total of accumulated savings or impacts for each of the above since the IWS was established.

Indicator #	Indicator	Disaggregated by gender	Guidance
			Note: Use forecasting models to estimate the financial value of risks mitigated by corrective actions.[11] Consider: • future losses avoided • fines or legal liabilities averted • reputational harm prevented, quantified where feasible • Opportunity costs mitigated, e.g. preserved funding, contracts.
28	**Appeals lodged by whistleblowers:** # of appeals lodged by whistleblowers, broken down by object of appeal: • the closure of the case, including referral to another procedure • the conduct or findings of any investigation actions • the conduct or outcome of the follow-up of the report • the measures taken by the organisation to address identified wrongdoing – or lack thereof – and their outcomes • limited or lack of feedback to a whistleblower • decision to disclose the identity of a reporting person without their consent.	Yes	**Record**, for each category of appeal, outcomes (founded or unfounded) and further actions taken.
29	**Appeals lodged by persons concerned:** # of appeals lodged by persons concerned, broken down by object of appeal: • non-respect of due process • the conduct or findings of any investigation actions • the conduct or the outcome of the follow-up to the report	Yes	**Record**, for each category of appeal, outcomes (founded or unfounded) and further actions taken.

[11] See, for example, Protect (2025), "The Cost of Whistleblowing – Assessing the cost of whistleblowing failures to the public purse", at https://protect-advice.org.uk/the-cost-of-whistleblowing-failures/.

Indicator #	Indicator	Disaggregated by gender	Guidance
	• the measures taken by the organisation to address identified wrongdoing, and their outcomes • a decision to disclose the identity of the person concerned without their consent.		
30	**Duration of follow-up of whistleblowing reports:** Breakdown of # of reports closed during the year, by length of follow-up (from reception to closure): • under 3 months • between 3 and 6 months • between 6 and 12 months • between 12 and 24 months • more than 24 months.		
31	**Initial feedback to whistleblowers:** Average time to provide whistleblowers initial feedback on the action(s) taken to follow up on their report.		**Record** instances where feedback was delayed or limited, and the reasons.
32	**Additional feedback requests:** Percentage of reports where whistleblowers requested additional feedback after initial feedback on action(s) taken to follow up on their report.		**Record** instances where additional feedback was refused or limited, and document the reasons.
33	**Whistleblowers' experience:** Rates of satisfaction reported by whistleblowers with: • the process overall • the reporting process • the follow-up or investigation process • the outcome of their cases • the frequency and quality of feedback received.	Yes	Requesting and analysing feedback from whistleblowers helps identify areas for improvement and build greater trust in the reporting process. For the overall process assessment, the whistleblower could be asked: "If your colleague were to witness wrongdoing, would you recommend that they use the IWS?" **Record** • # of whistleblowing reports where whistleblowers provided feedback on their experience

Indicator #	Indicator	Disaggregated by gender	Guidance
			• qualitative feedback on their experience and suggestions for changes in policy, procedures or processes.
34	**Changes to the IWS policies, procedures or processes resulting from feedback from whistleblowers**.		**Record** the weaknesses identified and action taken to address them.

INDICATORS ON COMPLAINTS OF DETRIMENTAL CONDUCT LINKED TO WHISTLEBLOWING

This section includes two sets of indicators. The first looks at complaints of detrimental conduct made internally to the organisation, while the second covers complaints of detrimental conduct lodged outside the organisation – including complaints for which an internal complaint was also made.

Indicators on complaints of detrimental conduct made internally to the organisation

Indicator #	Data on cases of detrimental conduct linked to whistleblowing	Disaggregated by gender	Guidance
1	**Retaliation complaints:** # of complaints of detrimental conduct received during the year.	Yes	
2	**Followed-up retaliation complaints:** Breakdown of # of complaints of detrimental conduct with follow-up during the year, by year of receipt of the complaint: • complaints received during the year • complaints received the year before • complaints received prior to the year before.		
3	**Retaliation complaints status:** Breakdown of # of complaints of detrimental conduct with follow-up during the year, by status of report at the end of the year: • complaints closed • complaints ongoing.		
4	**Initial assessment outcomes of retaliation complaints:** Outcome of initial assessment of complaints of detrimental conduct, for example: • initiation of internal investigation • referral to another internal complaint system • referral to a reporting or complaint system outside the organisation • closure with no further action taken • initial assessment still undergoing at year end.	Yes	

5	**Protective measures:** # of complaints where measures were taken to prevent further harm to the complainant (whistleblower or protected third party).	Yes	**Record** the type of measures taken.
6	**Outcomes of follow-up to retaliation complaint:** Breakdown of # of complaints of detrimental conduct followed up during the year by outcome: • no detrimental conduct was found, or there was insufficient evidence of detrimental conduct. • detrimental conduct was found to have occurred.	Yes	
7	**Types of retaliation:** # of instances of each type of detrimental conduct found to have occurred, for example: • dismissal or unjustified termination of contract • transfer or change of work duties; reduction in job responsibilities or quality of work, or demotion • disciplinary action • flawed, negative or no employment reference; blocklisting • poor or unfair performance review; denial of promotion, bonus or incentives • denial of benefits or perks due for any employee • coercion, intimidation, harassment or ostracism • breach of confidentiality in relation to the whistleblower's identity • initiation of unfounded external legal processes, such as a libel suit or criminal procedure for breach of confidentiality rules • physical harm or threats.	Yes	When deciding the categories of detrimental conduct into which the data should be broken down, organisations should take into consideration the types of detrimental measures covered, included those listed in the national law and the types of detrimental conduct covered by the organisation's anti-retaliation policy. **Note:** There can be more than one type of detrimental measure in a single case, meaning the same complaint can be counted several times.
8	**Retaliation remediations:** # of each type of action taken by the organisation to address proven detrimental conduct, for example: • reinstatement of the whistleblower or protected third party • voiding of detrimental measure taken against the whistleblower or protected third party (excluding reinstatement) • financial compensation of whistleblower or protected third party for damages • disciplinary proceedings against the perpetrator for misconduct.	Yes	**Note:** There can be more than one type of measure taken by the organisation to address the detrimental measure found in a single case, meaning the same complaint can be counted several times. **Record**:

			• which position the whistleblower was reinstated to, whether it was their original position, and if not, why • the average and total compensation amount • the types of measures made void • other remedies provided.
9	**Outcomes of disciplinary proceedings against the perpetrator of detrimental conduct**, by # of each type, for example: • warning • suspension • demotion • loss of benefits, salary deduction • transfer or reassignment • termination (dismissal) • legal action • # of disciplinary proceedings where no sanction was pronounced against the perpetrator of detrimental conduct.	Yes	Disaggregated data by gender of the whistleblower lodging the complaint, as well as of the person undergoing disciplinary proceedings, could provide useful information.
10	**Reductions to risk of retaliation:** Actions taken to correct a systemic issue identified, such as weaknesses in policy, procedure or controls, whether or not detrimental conduct was found.		**Record** the weaknesses identified and action taken to address them.
11	**Whistleblower and protected third-party appeals:** # of appeals lodged by complainants (whistleblower or protected third party), broken down by object of appeal: • the outcome of the initial assessment of the complaint of detrimental conduct • the conduct or findings of any investigation • the measures taken to prevent further harm to the complainant (or lack of such measures) • the conduct or outcome of the follow-up	Yes	**Record** for each category of appeal, outcomes (founded or unfounded) and further actions taken.

	• types of measures taken by the organisation to address identified detrimental conduct (or lack of such measures), and their outcomes.		
12	**Appeals by the person concerned:** # of appeals lodged by persons concerned, broken down by object of appeal: • non-respect of due process • the outcome of the initial assessment of the complaint • the measures taken to prevent further harm to the complainant, or lack of such measures • the conduct or findings of investigation actions • the conduct or outcome of the follow-up • the type of measures taken by the organisation to address identified detrimental conduct (or lack of such measures), and their outcomes.	Yes	**Record** for each category of appeal, outcomes (founded or unfounded) and further actions taken.
13	**Duration of follow-up to retaliation complaints:** Breakdown of # of complaints of detrimental measures closed at year-end, by length of follow-up (from receipt to closure): • under 3 months • between 3 and 6 months • between 6 and 12 months • between 12 and 24 months • more than 24 months.		
14	**Complainants' experience:** satisfaction rate reported by complainant whistleblowers and protected third parties with: • the process overall • the reporting process • the follow up or investigation process • the outcome of their case • the frequency and quality of feedback received.	Yes	Requesting and analysing feedback trends helps identify areas for improvement and build greater trust in the system. Organisations should collect feedback at the closure of the case, as well as after six months or a year, where possible. **Record:** • # of complaints of detrimental conduct where whistleblowers provided feedback on their experience

			• qualitative feedback on their experience and suggestions for changes in policy, procedures and processes.
15	**Changes to the complaint policies, procedures or processes following feedback from complainant whistleblowers or protected third parties.**		**Record** changes made and rationale behind the changes.

Indicators on complaints of detrimental conduct lodged outside the organisation

Indicator #	Complaints of detrimental conduct where the whistleblower took action outside the organisation	Disaggregated by gender	Guidance
16	**# of complaints of detrimental conduct where the whistleblower or protected third party lodged their complaint outside the organisation.**	Yes	
17	**External retaliation complaints and use of the organisation's complaint procedures:** Breakdown of the # of complaints of detrimental conduct where the whistleblower or protected third party lodged their complaint outside the organisation, by whether the complaint was also lodged internally: • # of complaints of detrimental conduct lodged outside the organisation after or in parallel to using the organisation's internal procedures • # of complaints of detrimental conduct lodged directly outside the organisation without using the organisation's internal procedures.	Yes	**Record** reasons why complainants lodged their complaints of detrimental conduct directly outside the organisation, without using its internal procedures where available.
18	**External complaint mechanism used:** Breakdown of # of complaints of detrimental conduct lodged outside the organisation by type of external complaint mechanism used, for example: • competent authority • employment tribunal • civil suit • criminal complaint • regulators or professional bodies	Yes	**Record** which authority, regulator or professional body, and the medium of public disclosures.

Indicator #	Complaints of detrimental conduct where the whistleblower took action outside the organisation	Disaggregated by gender	Guidance
	• other authorities not designated as competent for handling complaints of detrimental conduct, such as (depending on country) ombudspersons, human rights institutions, parliamentary bodies. • public disclosures, e.g. through the media, CSOs, social media.		
19	**Outcomes of external proceeding:** Breakdown of # of complaints of detrimental conduct lodged outside the organisation, by outcome: • no detrimental conduct was found, or there was insufficient evidence of such conduct, • detrimental conduct was found to have occurred.	Yes	
20	**Remediation for retaliation:** # of each type of measure recommended or ordered by external authorities to address identified detrimental conduct, for example: • reinstatement of the whistleblower • voiding of detrimental measure taken against the whistleblower (excluding reinstatement) • financial compensation of whistleblower for damages • other remedies • penalty for the individual who perpetrated detrimental conduct • penalty for the organisation.	Yes	**Record**: • which position the whistleblower was reinstated to, whether it was their original position, and if not, why • the types of measures made void • the average and total compensation amount • the penalties taken against individuals and the organisation • other remedies provided • reasons for not following the external authorities' recommendations.

INDICATORS ON AWARENESS OF AND TRUST IN THE ORGANISATION'S IWS

Indicator #	Data on awareness and trust in IWS	Disaggregated by gender	Guidance
1	**Training on the IWS:** • # and percentage of staff trained (excluding managers) • # and percentage of managers trained.	Yes	
2	Percentage of the organisation's workers who believe its leadership is ethical and supportive of the IWS.	Yes	Based on survey.
3	Percentage of the organisation's workers who, if they witnessed wrongdoing, would report it internally.	Yes	Based on survey.
4	Percentage of the organisation's workers who, if they witnessed wrongdoing, would report externally rather than internally.	Yes	**Record** reasons given by the respondent. Based on survey.
5	Percentage of the organisation's workers who understand which internal channel or mechanism to use for reporting concerns and wrongdoing.	Yes	Based on survey.
6	Instances where respondents indicated they reported wrongdoing externally.	Yes	**Record**: • reasons given by the whistleblower • whether the external report was made before, simultaneously or subsequently to the internal report. Based on survey.

7	Percentage of the organisation's workers who have experienced detrimental conduct after they reported wrongdoing.	Yes	More granular information can be collected – for example, by providing the following options to respondents: • dismissal or unjustified termination of contract • transfer or change of work duties; reduction in job responsibilities or quality of work, or demotion • disciplinary action • flawed, negative or no employment reference, blacklisting • poor or unfair performance review; denial of promotion, bonus or incentives • coercion, intimidation, harassment or ostracism • breach of confidentiality in relation to the whistleblower's identity • initiation of unfounded external legal processes, such as a libel suit or criminal procedure for breach of confidentiality rules • physical harm or threats.
8	Percentage of the organisation's workers who have observed detrimental conduct after a colleague reported wrongdoing.	Yes	More granular information can be collected – for example, by providing the following options to respondents: • dismissal or unjustified termination of contract • transfer or change of work duties; reduction in job responsibilities or quality of work, or demotion • disciplinary action • flawed, negative or no employment reference, blacklisting • poor or unfair performance review; denial of promotion, bonus or incentives • denial of benefits or perks that are due for any employee • coercion, intimidation, harassment or ostracism • breach of confidentiality over disclosure of the whistleblower's identity • initiation of unfounded external legal processes, such as a libel suit or criminal procedure for breach of confidentiality rules

			• physical harm or threats.
9	Percentage of the organisation's workers who have experience or observed negative changes in attitude towards themselves or a colleague who reported wrongdoing.	Yes	More granular information can be collected – for example, by providing the following options to respondents: • demeaning of work contribution • exclusion from meetings, or exclusion of input • exclusion from social events • pointed "gossip"; rude or disrespectful treatment • practical jokes • non-verbal harassment or bullying.
10	Recommendations from workers to improve the organisation's IWS.	Yes	Based on survey, with an open question to collect qualitative data.
11	# of individuals who used internal channels to obtain advice on the IWS.	Yes	
12	# of whistleblowers (named and unnamed) publicly commended for reporting wrongdoing.	Yes	

INDICATORS ON THE ORGANISATION'S RESOURCES FOR THE OPERATION OF ITS INTERNAL WHISTLEBLOWING SYSTEM

Indicator #	Resource Indicators	Disaggregated by gender	Guidance
Human resources			
1	Number and total accumulated full-time equivalents of personnel in the team responsible for operating the organisation's IWS.	Yes	**Record** the increase or decrease compared to the previous year.
2	Training personnel that are part of the team responsible for the operation of the organisation's IWS.	Yes	**Record** the number and type of training courses attended by the IWS personnel, as well as the training courses available to them during the past three years.
3	Number, description and cumulated days of work of external consultants or advisors engaged for the operation of the organisation's IWS.	Yes	**Record** the increase or decrease compared to the previous year.
4	# of whistleblowing reports where external experts were contracted by the organisation as part of its investigation, e.g. auditors, legal professionals.	Yes	**Record** the type of external experts and overall costs of these experts.
5	Level of confidence of designated persons within the IWS, including report recipients, in their capacity to handle cases effectively.		**Record** any increase or decrease compared to previous years.
Financial resources			
6	Total budget and portion of the organisation's budget for the year reported, broken down by: • training and awareness raising • investigation and follow up • whistleblower support and protection • system maintenance and upgrades • other.		**Record** increase or decrease compared to the previous year.

7	Total spending during the year reported, broken down by projected and actual spending on: • training and awareness • investigation and follow-up • whistleblower advice, support and protection • system maintenance and upgrades • other.		**Record** increase or decrease compared to the previous year.
Technological resources			
8	Description of technological tools utilised, e.g. online reporting platform, case management systems.		**Record** upgrades made during the year, any complaints made about the system and any hours of downtime, as well as feedback on the use of technological tools.

RESOURCES

FROM TRANSPARENCY INTERNATIONAL

Marie Terracol (2022), *Internal Whistleblowing Systems – Best practice principles for public and private organisations*, https://www.transparency.org/en/publications/internal-whistleblowing-systems.

Marie Terracol (2024), *Internal Whistleblowing Systems – Self-Assessment Framework for public and private organisations*, https://www.transparency.org/en/publications/internal-whistleblowing-systems-self-assessment-framework-public-private-organisations.

Jacqueline de Gramont (2017), *The Business Case for "Speaking Up": How Internal Reporting Mechanisms Strengthen Private-Sector Organisations*, Transparency International, www.transparency.org/en/publications/business-case-for-speaking-up.

Transparency International and World Economic Forum (2024), *Business Integrity: A Toolkit for Medium-Sized Enterprises*, https://images.transparencycdn.org/images/TI-Business-Integrity-Toolkit.pdf.

Transparency International, *Anti-Corruption Toolkits for Business*, https://www.transparency.org/en/toolkits/business.

Peter Wilkinson (2017), *10 Anti-Corruption Principles for State-Owned Enterprises*, Transparency International, www.transparency.org/en/publications/10-anti-corruption-principles-for-state-owned-enterprises.

Marie Chêne (2021), "Finding a voice, Seeking Justice – the barriers women face to reporting corruption in the European Union", Position Paper, Transparency International, www.transparency.org/en/publications/finding-voice-seeking-justice-barriers-women-face-reporting-corruption-european-union.

Transparency International Ireland (2021), *National Integrity Index 2021, Public-Sector Bodies (Part 1), Semi-States and Universities*, www.transparency.ie/resources/national-integrity-index/semi-state-universities-index-2021/report.

Dr Roland Gjoni (2021), *National Integrity Index 2020, Private Sector: Assessing Disclosure Practices of 30 Irish Companies*, Transparency International Ireland, www.transparency.ie/resources/national-integrity-index/private-sector-index/report-2020.

Transparency International Helpdesk Answers

Caitlin Maslen (2023), "Responses to common challenges encountered when establishing internal whistleblowing mechanisms", https://knowledgehub.transparency.org/helpdesk/responses-to-common-challenges-encountered-when-establishing-internal-whistleblowing-mechanisms.

Matthew Jenkins (2020), "Overview of whistleblowing software", U4 Helpdesk Answer, Transparency International, https://knowledgehub.transparency.org/helpdesk/overview-of-whistleblowing-software.

Kaunain Rahman (2018), "The impact of General Data Protection Regulation on whistleblowing", Transparency International, https://knowledgehub.transparency.org/helpdesk/the-impact-of-the-general-data-protection-regulation-on-whistleblowing.

OTHER RESOURCES

International Organization for Standardization (ISO) (2021), *Whistleblowing management systems — Guidelines*, ISO 37002:2021.

Protect (2022), *Prescribed Persons – Annual Whistleblowing Reports: Best Practice Guide, https://public-concern-at-work.s3.eu-west-1.amazonaws.com/wp-content/uploads/images/2022/08/30095958/Annual-Whistleblowing-Reports-Best-Practice-Guide.pdf*.

Protect (2025), *The Cost of Whistleblowing – Assessing the cost of whistleblowing failures to the public purse*, https://protect-advice.org.uk/the-cost-of-whistleblowing-failures/.

International Chamber of Commerce (2022), Guideline on Whistleblowing, https://iccwbo.org/publication/icc-2022-guidelines-on-whistleblowing/.

United Nations Office on Drugs and Crime (2021), *Speak Up for Health! Guidelines to enable whistle-blower protection in the health-care sector*, www.unodc.org/documents/corruption/Publications/2021/Speak_up_for_Health_-_Guidelines_to_Enable_Whistle-Blower_Protection_in_the_Health-Care_Sector_EN.pdf.

Organisation for Economic Co-operation and Development (2021), *Recommendation of the Council for Further Combating Bribery of Foreign Public Officials in International Business Transactions*, OECD/LEGAL/0378, www.oecd.org/corruption/2021-oecd-anti-bribery-recommendation.htm.

Vigjilenca Abazi (2021), *Guide to Internal Whistleblowing Channels and the Role of Trade Unions*, Eurocadres, www.eurocadres.eu/publications/guide-internal-whistleblowing-channels-and-the-role-of-trade-unions.

Kai-D Bussmann, Sebastian Oelrich, Andreas Schroth, Nicole Selzer, *The Impact of Corporate Culture and CMS: A Cross-Cultural Analysis on Internal and External Preventive Effects on Corruption* (Springer Cham, 2021).

European Parliament and Council of the European Union (2019). *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*, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32019L1937.

European Data Protection Supervisor (2016), *Guidelines on processing personal information within a whistleblowing procedure*, https://edps.europa.eu/data-protection/data-protection/reference-library/whistleblowing_en.

Principles for Responsible Investment (2020), Whistleblowing: Why and how to engage with investee companies, https://www.unpri.org/sustainability-issues/environmental-social-and-governance-issues/governance-issues/whistleblowing.

Stephen Stubben and Kyle Welch (2020), "Evidence on the Use and Efficacy of Internal Whistleblowing Systems", *Journal of Accounting Research,* Volume 58, Issue 2, 473-518.

Bussmann, K-D. and 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.

ACKNOWLEGEMENTS

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

Adam Foldes, Transparency International

Alessia Rizzo, Transparency International Italia

Annie Healion, Transparency International

Caitlin Malsen, Transparency International

Celine Pinzio, Transparency International

Giorgio Fraschini, Transparency International Italia

Giovanni Pellerano, Whistleblowing Solutions

Irina Lonean, Transparency International Romania

Jan Dupák, Transparency International Czechia

John Devitt, Transparency International Ireland

Judit Zeisler, Transparency International Hungary

Kremena Chobanova, Transparency International Bulgaria

Laurence Fabre, Transparency International France

Lotte Rooijendijk, Transparency International Netherlands

Susanna Ferro, Whistleblowing Solutions

ENGAGE

Follow us, share your views and discuss corruption with people from around the world on social media.

@anticorruption.bsky.social

/transparencyinternational

@anticorruption

@transparency-international

@Transparency_International

@transparency_international

@TransparencyIntl

LEARN

Visit our website to learn more about our work in more than 100 countries and sign up for the latest news in the fight against corruption.

transparency.org

DONATE

Your donation will help us provide support to thousands of victims of corruption, develop new tools and research, and hold governments and businesses to their promises. We want to build a fairer, more just world. With your help, we can.

transparency.org/donate

Transparency International
International Secretariat
Alt-Moabit 96, 10559 Berlin, Germany

Phone: +49 30 34 38 200

ti@transparency.org
www.transparency.org


@anticorruption.bsky.social


/transparencyinternational


@anticorruption


@transparency-international


@Transparency_International


@transparency_international


@TransparencyIntl