



Whistleblower
Empowerment
& Support Initiative



Co-funded by
the European Union

Skills Assessment Report

Evaluating Organizational Capacity
in Whistleblower Protection

Project co-funded by the European Union through the European Commission - Citizens, Equality, Rights and Values Programme (CERV)



Grant Agreement number:	101213588
Project acronym:	VoiceGuard
Project title:	VoiceGuard: Whistleblower Empowerment & Support Initiative
Call:	CERV-2024-CHAR-LITI
Duration:	24 months
Start date:	01/06/2025

DISCLAIMER

Funded by the European Union. Views and opinions expressed in this Deliverable are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for the content.

STATEMENT OF ORIGINALITY: This deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation, or both.

COPYRIGHT: This work is licensed by the VoiceGuard Consortium under a Creative Commons Attribution-ShareAlike 4.0 International License. For details, see <https://creativecommons.org/licenses/by-sa/4.0/>

1. Introduction	4
2. Methodology	5
2.1. Research Design and Objectives	5
2.2. Data Collection	5
2.3. The Analytical Framework	5
3. Analysis	7
3.1. The Information Ecosystem	7
3.1.1. Accessibility and Visibility of Information	7
3.1.2. Quality of Publicly Available Information	8
3.1.3. Types of Reportable Conduct	9
3.1.4. Training Frequency for Regular Employees	10
3.2. Reporting Channels and Functional Independence	10
3.2.1. 7-Day Acknowledgment Compliance	10
3.2.2. Reporting Channels	11
3.2.3. Handling of Anonymous Reports	12
3.2.4. Perceived Functional Independence	13
3.2.5. Legal Assessment Complexity	14
3.3. Feedback Quality and Whistleblower Protection Mechanisms	15
3.3.1. Feedback Provision Models	16
3.3.2. Whistleblower Engagement in Follow-up Measure Identification	18
3.3.3. Active Retaliation Prevention	18
3.4. Resources and Professionalization	20
3.4.1. Human Resource Allocation	20
3.4.2. Staffing and Gender Balance	21
3.4.3. Training Frequency for Persons Responsible for IRS	23
3.5. Requested Support and Country-Specific Perspective	25
3.5.1. Requested Support	25
3.5.2. Country-Specific Perspective	26
4. Conclusion	29

1. Introduction

Individuals who report wrongdoing play a crucial role in exposing corruption and other forms of misconduct that threaten public welfare. Whistleblowers have contributed to safeguarding lives and conserving public resources through their disclosures. However, those who disclose such information often face significant personal risks, including loss of employment, workplace harassment, exclusion from future opportunities, and, in extreme cases, physical harm.

Protecting whistleblowers from unjust consequences, including retaliation, discrimination, or other adverse actions, encourages greater reporting of misconduct. Such protection increases the likelihood that wrongdoing will be prevented, detected, and sanctioned. Therefore, safeguarding individuals who report wrongdoing is essential for enhancing legal compliance.

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 (hereinafter “Directive”), became effective on December 16, 2019, with a transposition deadline of December 17, 2021. Although many Member States did not meet this deadline, implementation accelerated in 2022 and 2023 following infringement proceedings by the European Commission. By the end of 2023, all EU Member States had enacted national legislation to implement the Directive, although the speed and quality of transposition varied significantly. Under the principle of direct effect, public sector entities have been subject to the Directive’s obligations since December 17, 2021, while private sector obligations commenced upon national implementation in each Member State.

The VoiceGuard project, funded by the Citizens, Equality, Rights and Values Programme (CERV), seeks to enhance the implementation and effectiveness of whistleblower protection throughout the European Union. Work Package 2 constitutes the analytical core of the project and includes a Needs Analysis, a Skills Assessment, a Best Practice Analysis, and a Policy Recommendations Report. Collectively, these components establish a comprehensive evidence base to identify gaps, build capacity, and develop practical tools for improving whistleblower protection systems.

This Skills Assessment Report focuses on organizational ability, namely organizational skills and competences of those responsible for handling and receiving reports. A 21-question questionnaire has been applied in six target Member States: Bulgaria, Czech Republic, Spain, Greece, Luxembourg, and Romania. This research seeks to analyze gaps creating the disconnect between the official legal implementation of Union law and the practical skills of those responsible for its execution on an organizational level.

2. Methodology

2.1. Research Design and Objectives

The core of this research is a 21-question questionnaire specifically developed to evaluate the skills and competencies of personnel responsible for receiving and handling reports. By focusing on four key areas: transparency, accessibility, identity protection, and feedback quality, the questionnaire identifies the organizational maturity in protecting whistleblowers and addressing misconduct effectively.

2.2. Data Collection

The data collection took place in six EU member states. The questionnaire was translated into seven languages and distributed across six EU member states. The data collection was conducted over a two-month period, from December 1, 2025, to January 31, 2026, yielding a total sample size of 150 respondents.

Geographical Distribution:

- Bulgaria: 32 responses
- Czech Republic: 30 responses
- Spain: 29 responses
- Greece: 24 responses
- Luxembourg: 20 responses
- Romania: 15 responses

The respondents represent primarily the Public sector (public authority, public institution, municipal or regional self-government) (50.7%), followed by legal entities with state or municipal or regional ownership participation (33.3%), for-profit business corporations (6%), and non-profit or non-governmental organization (3.33%).

Based on an audit of the 150 respondents in the diagnostic dataset, 19.3% operate in more than one country. The questionnaire provided a definition to ensure data consistency: “By ‘operate in more than one country’ is meant that the organization has offices, branches, subsidiaries, or regular activities in at least two countries. Occasional business trips or individual diplomatic postings do not count.”

2.3. The Analytical Framework

The analysis is structured around five sections.

The information ecosystem section has a primary objective in determining whether reporting channels are functionally visible or exist as administrative outliers. It evaluates the accessibility and clarity of the system, analyzing how organizations integrate the internal reporting systems (IRS) into their culture. Furthermore, this section assesses the material scope of reportable conduct in organizations and examines the frequency of training of regular employees.

The second section, Reporting Channels and Functional Independence, examines the operational machinery of the internal reporting systems (IRS). It evaluates whether an organization's procedures, ranging from the initial intake of a report to the structural autonomy of the investigators, are robust and timely enough to ensure an impartial examination of wrongdoing. The analysis begins by assessing the accessibility of reporting channels and the organization's discipline in meeting the statutory 7-day acknowledgment deadline, alongside a review of the protocols for handling anonymous disclosures. Subsequently, it focuses on the capacity of the person responsible for managing the IRS to operate with functional independence and sufficient power to investigate sensitive cases without hierarchical interference.

The third section, Feedback Quality and Whistleblower Protection Mechanisms, evaluates the quality of feedback provided to the whistleblower and the active protective measures implemented within the IRS. The quality of feedback is the primary determinant of whistleblower trust. The analysis evaluates the quality of communication, contrasting strict adherence to minimum obligations with proactive engagement. Crucially, it assesses whether whistleblowers are treated as passive data sources or as informed partners in remediation, measuring whether proposed follow-up measures are discussed and jointly reviewed. Finally, it examines the protective infrastructure, such as the presence of active retaliation monitoring and psychosocial support mechanisms.

In section 4, focusing on resources and professionalization, we map the human resources dedicated to IRS, using the Full-Time Equivalent (FTE) allocation as a primary indicator. Beyond time allocation, this section evaluates the gender diversity of the persons responsible for receiving and handling reports, one of best-practice metrics for ensuring IRS accessibility. The analysis concludes by identifying the training frequency for persons responsible for IRS management.

In the final fifth section, we analyze the data regarding which forms of support respondents explicitly indicated they would welcome to further develop their internal reporting systems. Finally, we apply a country-specific perspective to this data to uncover local demands in the area of internal whistleblower protection.

3. Analysis

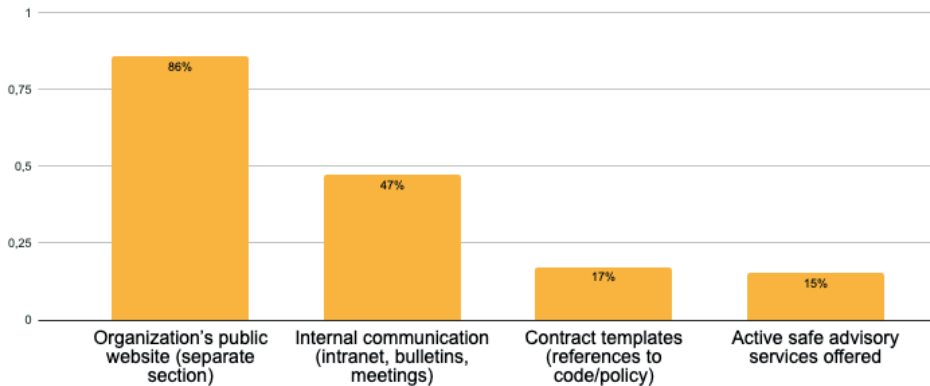
3.1. The Information Ecosystem

This section evaluates the visibility and clarity of an organization’s Internal Reporting System (IRS). A functional information ecosystem is the primary mechanism for promoting the speak-up culture by ensuring that the workforce understands what to report, how to do so safely, and where to find the statutory protections guaranteed by Directive (EU) 2019/1937.

3.1.1. Accessibility and Visibility of Information

The methods organizations use to disseminate information about their internal reporting systems offer a first glance into the organizational culture and show the approach which organization has towards its whistleblowers.

How and where does your organization provide information about its internal reporting system (IRS)



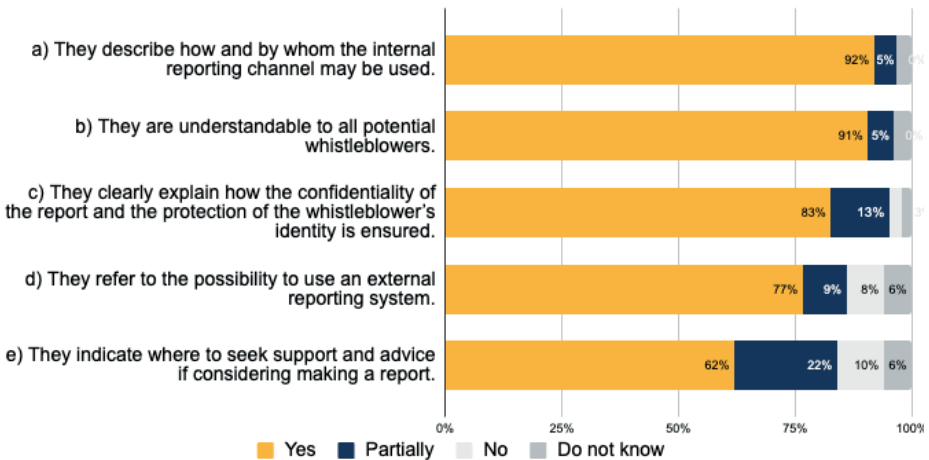
Note: Based on 150 respondents in the source dataset; respondents could select multiple options.

The data shows that almost 9 of 10 respondents (86%) comply with the Directive’s requirements to publish information about their internal reporting system on a public website. Approximately half of all organizations communicate this information internally, i.e., through meetings, bulletins, or intranets. When it comes to utilizing more advanced methods to transparently communicate the IRS function, the numbers drop significantly: only 17.3% of respondents include IRS references in contract templates, and just 15.3% offer active safe advisory services—suggesting that true whistleblower protection maturity is limited to this small group. In fact, the adoption of at least one of these advanced methods is seen in only 35 organizations.

3.1.2. Quality of Publicly Available Information

While organizations largely fulfill the Directive’s mandate to publish information online, this practice can evolve from compliance issues into a tool for building trust. Effectively published information should clearly explain the reporting process, whistleblowers rights, confidentiality protocols, and external support options to help whistleblowers determine if their disclosure is protected.

Do the following statements apply to publicly available information about your organization’s internal reporting system?



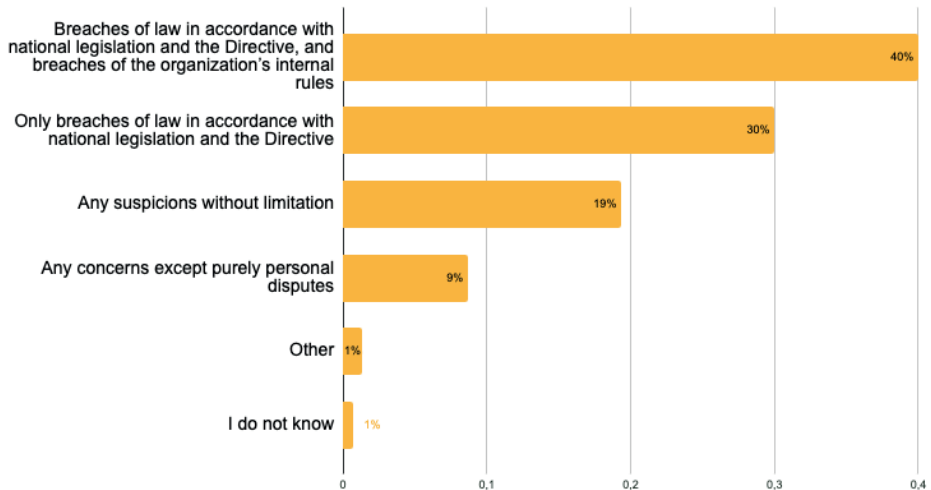
While 92% of organizations claim their public information is understandable, clarity drops to 83% regarding whistleblower identity protection, suggesting a focus on process over whistleblower rights.

A reference to the external reporting system (an obligation under Directive) is fully present in 77% of respondents and indication of where to seek support is fully met by 62% of our respondents and partially by additional 22%, as you can see in the following graph. Further 8% of organizations fail to inform employees about external reporting channels and an additional 4% do not know whether they comply with this metric. Whether this is a result of negligence or a deliberate strategy to restrict disclosures to internal reporting, this would constitute a breach of the Directive. Article 9(1)(c) mandates that organizations must make information regarding external reporting procedures clear and easily accessible.

3.1.3. Types of Reportable Conduct

Beyond the quality of information provided to employees, organizations in the selected member states retain the right to voluntarily broaden the material scope of what may be reported via their Internal Reporting Systems (IRS). However, expanding the IRS does not automatically extend statutory protection to all disclosures. Since whistleblower laws specifically define protected reports based on the subject matter (e.g., breaches of EU or national law), reports concerning only internal guidelines or ethical codes often fall outside the statutory safety net. Nevertheless, broadening the scope of reportable conduct is highly beneficial: it reduces confusion, simplifies navigation for the whistleblower, and significantly strengthens the organization's 'speak-up' culture, as it removes the burden on potential whistleblowers to determine if a concern meets complex legal criteria before speaking up.

According to publicly available information about your internal reporting system, what types of conduct can be reported via the internal reporting channel?



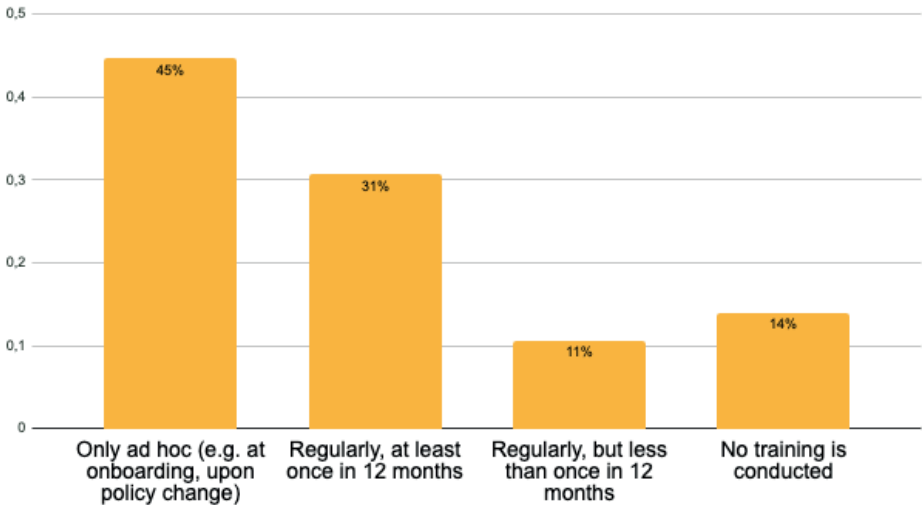
Nearly one-third of organizations limit reporting strictly to the legal minimum mandated by Directive and national legislation. This often creates a chilling effect where employees who are not fully certain their concern fits narrow legal criteria remain silent to avoid the risk of retaliation for an unprotected report. A slightly broader group of 40% of respondents also accept reports on breaches of internal regulations.

The remaining group of organizations allowing for reporting of any concerns without limitation (19%) or any concerns with the limitation of strictly personal disputes (9%) represents a combined over 1/4 of respondents with a more mature speak up culture.

3.1.4. Training Frequency for Regular Employees

When staff are trained, they are more likely to recognize reportable conduct. Furthermore, on-going education acts as a safety net by teaching colleagues how to avoid accidentally isolating or bullying those who speak up.

How often does your organization train regular employees on reporting procedures?



The data reveal that the largest group of organizations (45%) relies exclusively on ad hoc training (i.e. during onboarding). This one-and-done approach fails to reinforce the mechanism, supporting the often default culture of silence. When combined with the 14% of respondents who report ‘no training conducted,’ nearly 60% of employees operate in an environment where awareness is insufficient to identify reportable conduct.

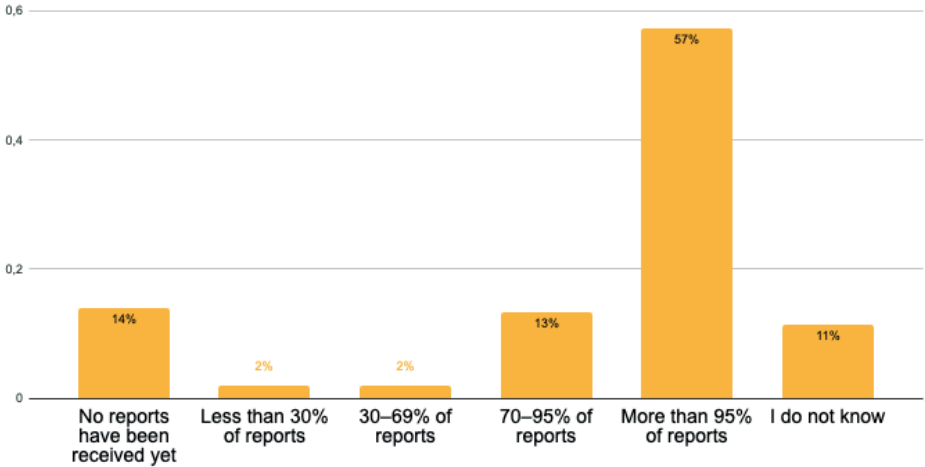
In contrast, over a third of organizations provide regular training at least annually. Such recurring education is essential to normalize whistleblowing, transforming it into a standard workplace tool.

3.2. Reporting Channels and Functional Independence

3.2.1. 7-Day Acknowledgment Compliance

The acknowledgment of receipt of the report within seven days is an obligation under the Directive. The following question tested the compliance rate with this obligation and at the same time uncovered how many organizations are yet to receive their first whistleblower report.

For approximately what percentage of reports do you acknowledge receipt to the reporter within 7 days?



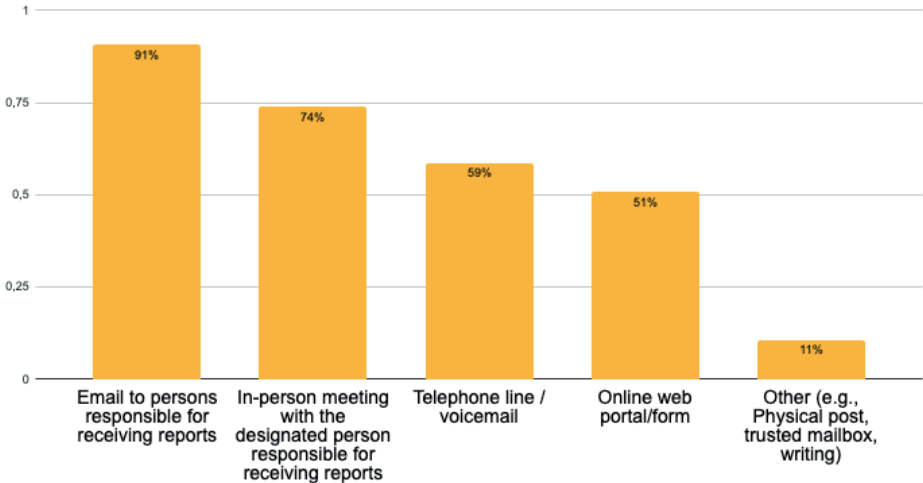
Organizations meeting the statutory 7-day acknowledgement deadline for more than 95% of reports account for 57.3% of the sample (86 out of 150). Within this compliance group, 62.8% (54 organizations) provide an online web portal, facilitating often automated confirmation of receipt mandated by Article 9 of Directive (EU) 2019/1937.

For the 17% struggling with compliance with the Directive and 11% that answered I do not know, there is a high risk of reports entering an institutional void. Whether intentionally or not, this inaction demoralizes the whistleblower and signals organizational apathy. The Directive itself states in recital 63 that lack of confidence in the effectiveness of reporting is one of the main factors discouraging potential whistleblowers.

3.2.2. Reporting Channels

The Directive mandates that Internal Reporting Systems (IRS) enable reporting both in writing and orally, including via telephone or other voice messaging systems, and—upon request—by means of a physical meeting. Secure online web portals or forms can provide an additional layer of security, allow for automated responses, facilitate easier case management, and crucially, sometimes enable two-way anonymous communication repeatedly recommended by experts.

What reporting channels does your organization offer?



Over half of the organizations surveyed (50.7%) provide either a web portal or an online form, suggesting a shift toward a more professional and secure approach to handling disclosures. However, the data simultaneously reveal a significant breach of the Directive: Despite the legal requirement to facilitate physical meetings upon request pursuant to Article 9 (2) of the Directive, only 74% of organizations explicitly list physical meetings as an available channel. This indicates that 26% of organizations are non-compliant with the mandatory provision to offer face-to-face reporting.

According to our data, the presence of an online portal significantly increases the likelihood of secure interaction. While 40.3% of organizations with online web portals (77) facilitate two-way anonymous communication, that figure drops to just 6.8% for a group of organizations without online web portals or forms. This suggests that without dedicated digital tools, most organizations are unable to maintain an anonymous dialogue with the reporter.

3.2.3. Handling of Anonymous Reports

While the Directive grants Member States the discretion to decide whether to accept anonymous reports, Article 6 explicitly mandates that anonymous whistleblowers who are subsequently identified must be protected from retaliation. As national legislations rarely extend protection beyond this minimum, the practical responsibility for defining how anonymous reports are handled falls upon individual organizations. Regardless of the approach chosen, it is highly advisable that organizations maintain evidence of anonymous reports to ensure legal compliance should the whistleblower's identity be revealed later.

How does your organization handle anonymous reports?



Note: Total exceeds 100% as respondents could select multiple options.

The data indicate a polarized landscape. On the one hand, 42% of organizations treat anonymous reports as standard non-anonymous reports, and 22.67% have implemented two-way anonymous communication. These figures prove the existence of maturing organizational culture that prioritizes the content of the report over the identity of the reporter. However, for an anonymous investigation to be truly effective, the ability to ask follow-up questions is critical; investigating without a feedback loop can lead to dead ends.

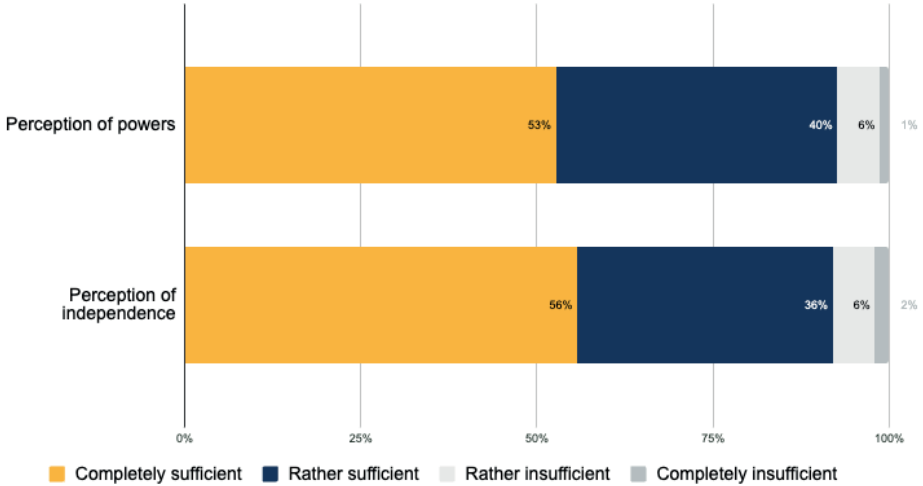
On the other hand, 26% of organizations refuse anonymous reports entirely and 18.67% (28 organizations) that condition investigation on sufficient supporting information. Crucially, of these 28 organizations requiring sufficient information, only 9 enable two-way communication. This creates a procedural trap: the organization may often demand more evidence to proceed, but provides no safe channel for the whistleblower to submit it. By refusing anonymous reports or setting static evidence thresholds without the possibility of dialogue, organizations inadvertently filter out valid concerns before they can be understood or verified.

3.2.4. Perceived Functional Independence

For whistleblowing systems to be effective, the individuals responsible for receiving and handling reports must be organizationally independent and possess the capacity to conduct impartial investigations. Without these safeguards, whistleblowers often fear that their identities will be exposed or that the reported wrongdoing will be covered up by the very people tasked with investigating it. Because organizations have the discretion to decide exactly what level of independence to grant, the autonomy of the person responsible for receiving and handling reports is a major sign of how mature the organizational culture actually is.

Correlation of Perceived Independence and Perceived Powers

Do you consider the independence/power of person(s) responsible for the IRS sufficient for impartial examination of reports, including those concerning senior officials?

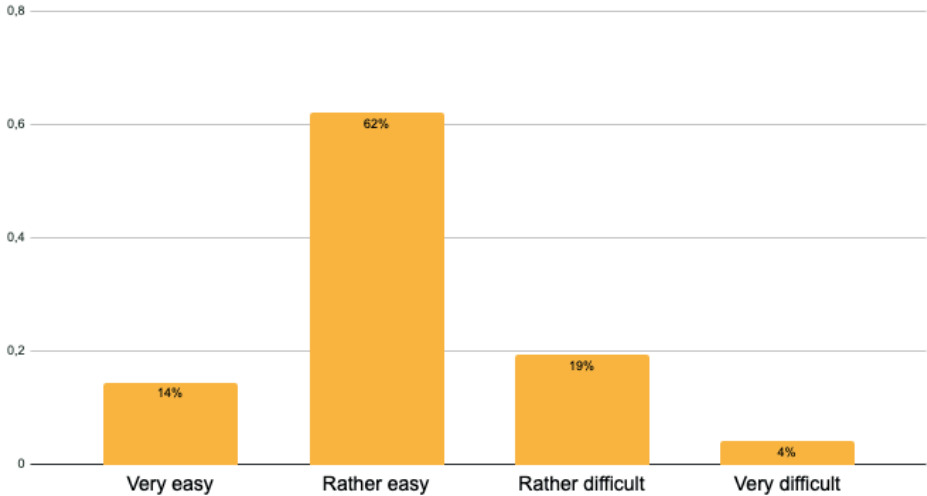


The data reveal a nearly identical statistical alignment between an officer’s perceived independence and their perceived power to examine reports, including those concerning senior officials. Most respondents (56%) feel their independence is completely sufficient, though this must be viewed in light of the resource constraints mentioned above. Over one-third of officers operate in a state of ambiguity, stating their power and independence is only rather sufficient, implying they may remain subordinate to the very management they are meant to oversee. The minority of 8% organizations reported insufficient independence and 7% insufficient powers.

3.2.5. Legal Assessment Complexity

The legal assessment of whether a report falls under the scope of whistleblower protection legislation constitutes a significant hurdle for both whistleblowers and the persons responsible for receiving and handling reports. Whistleblowing frameworks are often fragmented and legally complex, particularly regarding the material scope of the EU Whistleblower Protection Directive which covers only specific areas of Union law. This complexity makes it difficult for workers without advanced legal expertise to determine if the misconduct they witness is actually protected. If a report is incorrectly assessed as falling outside the legal scope, the whistleblower is left disoriented and vulnerable to retaliation without the statutory safeguards they anticipated.

How difficult is it for you from a legal standpoint to assess whether a report falls under the scope of the Directive or national whistleblower protection law?



Despite these complexities, the largest portion of the sample perceives this task as manageable. When combined, those who find it very easy or rather easy to assess the material scope make up 76% of the respondents. However, nearly a quarter of the respondents fall within the rather difficult or very difficult categories. While the confidence among the majority is a positive sign, a 23% rate of those who find legal assessment difficult is a concerning sign of potential errors in distinguishing between a protected disclosure and other disputes. Where uncertainty exists, organizations are more likely to default to report suppression rather than investigation.

This also points to a significant capacity gap, potentially placing organizations in non-conformity with the Directive's Article 9 requirement for competent persons to handle reports. If nearly one in four officers struggles to identify protected speech, the organization cannot guarantee the correct application of the law. Furthermore, uncertainty about legal thresholds may prevent designated persons from supporting the speak-up culture in their organizations.

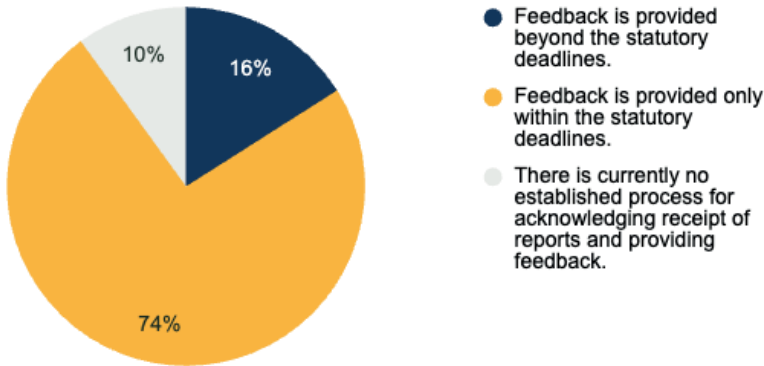
3.3. Feedback Quality and Whistleblower Protection Mechanisms

This pillar evaluates the „Feedback Loop“ and the active protective measures implemented within Internal Reporting Systems (IRS). The quality of feedback is the primary determinant of whistleblower trust; the process of being heard is often more significant than the final outcome of an investigation in building long-term organizational integrity.

3.3.1. Feedback Provision Models

Effective communication is the only tangible evidence a whistleblower has that their report is being taken seriously; without it, the silence following a disclosure is often interpreted as inaction or indifference. We asked organizations to categorize their approach to this critical dialogue, distinguishing between those that strictly adhere to the minimum legal requirements and those that prioritize ongoing engagement. This higher standard of feedback involves communicating beyond the statutory deadlines, for example, by providing interim updates on the status of the investigation or keeping the reporter informed as the case moves through different procedural stages.

How is feedback provided to the reporter after submitting a report?

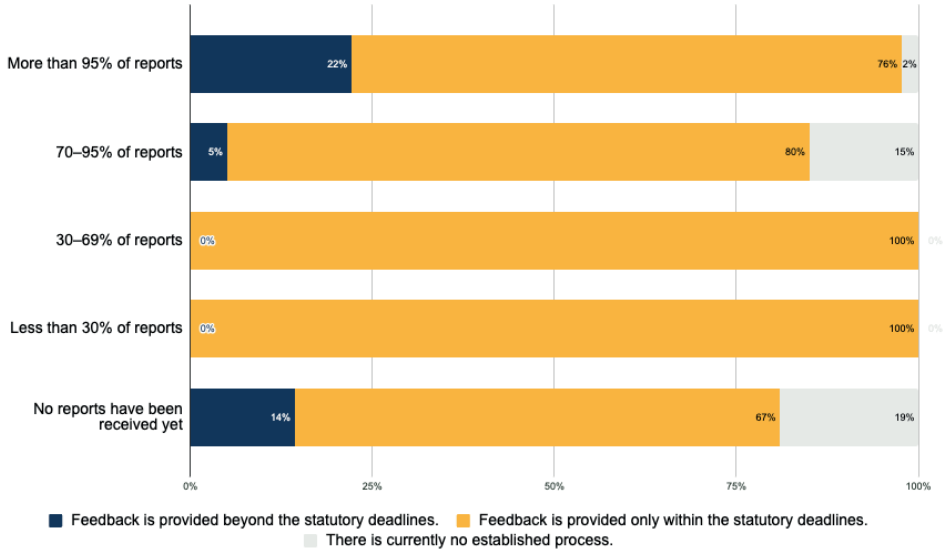


The manner in which an organization provides feedback to a reporter reveals whether they view compliance as a checklist or a commitment to trust. The data indicates that 74% of organizations treat the requirements of Directive (EU) 2019/193, specifically the seven-day acknowledgment and three-month feedback window, as a ceiling rather than a floor. By adhering strictly to these statutory deadlines without offering further engagement, the vast majority of entities miss the opportunity to foster a supportive environment.

In contrast, only 16% of organizations provide ongoing updates beyond the statutory minimum, maintaining active communication regarding the status of the investigation and next steps. This proactive approach is crucial, as silence is often perceived by the whistleblower as indifference or even the first stage of retaliation.

The remaining 10% of respondents admitted to having no established process for acknowledging receipt or providing feedback. Far from being insignificant, this figure represents a critical failure in compliance. Beyond constituting a direct breach of the Directive, this lack of structure signals that one in ten organizations struggles with the capacity to understand and implement even their most basic legal obligations.

Acknowledgement speed vs. Feedback Depth



When we compare how organizations claim to be successful at acknowledging the receipt of a report in 7 days with how feedback is provided throughout the process, the data reveals a correlation. 22% of organizations that maintain a perfect or near-perfect acknowledgment rate (acknowledging more than 95% of reports within the 7-day statutory limit) also implement ongoing dialogue models that extend beyond legal deadlines.

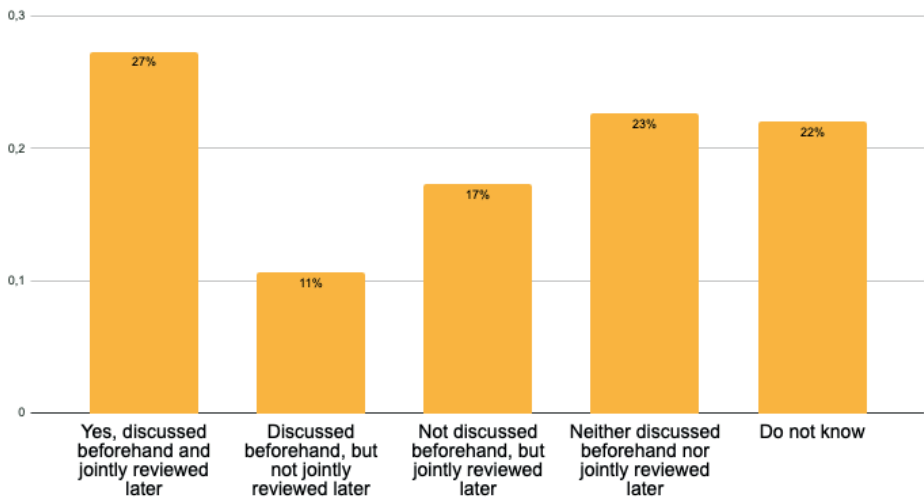
Further, there is a significant overlap between organizations that have not received any reports and those that admit to having no currently established process (19%). This suggests a self-filling prophecy: the absence of reports in these organizations is likely not a reflection of a pristine environment, but rather the result of failing to implement a functional, accessible mechanism for reporting.

The anomaly where 14% of organizations with zero history of reports claim to exceed statutory feedback standards suggests a case of aspirational compliance. Since these entities have never actually processed a report, their claim reflects their internal policy or personal intention rather than reality.

3.3.2. Whistleblower Engagement in Follow-up Measure Identification

Engaging the whistleblower in the decision-making process is a strategic asset for both the individual and the organization. It is usually the whistleblower who possesses the specific, on-the-ground understanding of the workplace complexity and the reported issue; therefore, their input is essential for ensuring that follow-up measures are effective.

Are proposed follow-up measures discussed with the reporter before implementation and then jointly reviewed after a certain period?

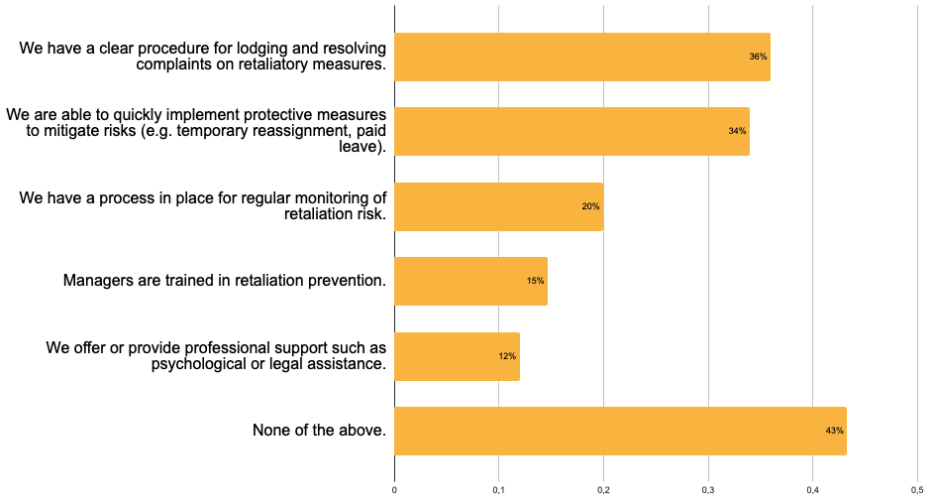


The data shows that 27% of organizations represent the gold standard of speak-up culture maturity in setting up follow-up measures. By pre-discussing proposed solutions and jointly reviewing their implementation, these organizations treat the whistleblower as an informed stakeholder rather than a passive data source. In contrast, 23% of organizations operate a closed system that excludes the reporter from any engagement in solution finding or approval. Between these two extremes, organizations show a preference for retrospective validation over proactive consultation. Interestingly, organizations are more likely to review follow-up measures with the whistleblower after implementation (17%) than to discuss them before implementation (11%). This suggests that organizations remain hesitant to share decision-making power during the formulation phase.

3.3.3. Active Retaliation Prevention

A true measure of a protective system is its ability to shield the whistleblower from harm after the disclosure is made. To assess the maturity in this aspect, we asked organizations a direct question regarding their prevention mechanisms.

How does your organization prevent retaliatory measures and support whistleblowers?



Note: Based on 150 respondents in the source dataset; respondents could select multiple options.

The data regarding active retaliation prevention exposes that 43.3% of organizations offer zero analyzed types of active support. This confirms a minimalistic approach to whistleblower protection from or in the case of retaliation. The absence of any visible safety nets signals to employees that they report at their own risk.

Among the organizations that do provide some form of mechanism, there is a distinct preference for passive, reactive tools over active prevention. While 36% of respondents have established clear procedures for lodging complaints about retaliation, only 20% have implemented a process for the regular monitoring of retaliation risks. This reactionary stance is further evidenced by the low priority given to education since only 14.7% of organizations train their managers in retaliation prevention. Consequently, organizations are far better equipped to process a retaliation claim after the damage is done than they are to identify and stop the behavior before it escalates.

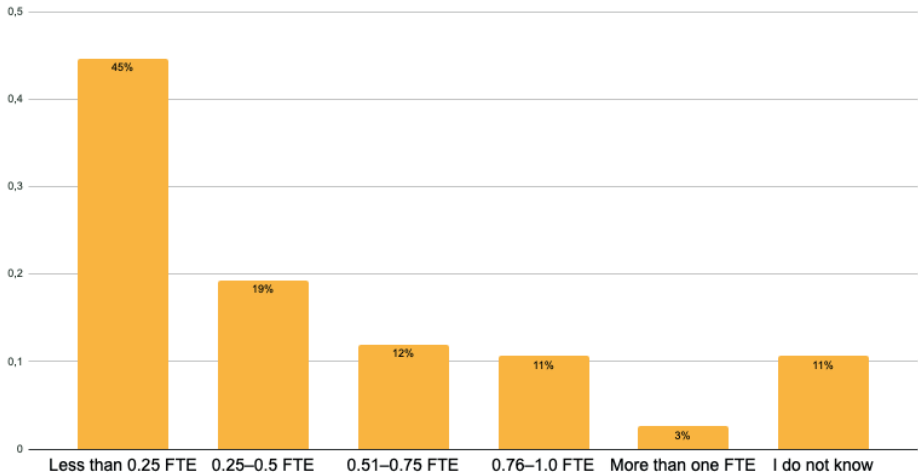
Furthermore, the human element of whistleblowing is largely neglected. Only 12% of respondents offer professional support, such as psychological or legal assistance. This critically low figure confirms that in the vast majority of cases, whistleblowers are left to bear the emotional and financial burden of their disclosures alone, forced to seek advice externally through paid professional services or non-governmental organizations.

3.4. Resources and Professionalization

3.4.1. Human Resource Allocation

The effectiveness of an internal reporting system is determined also by the human resources engaged in its operation. We analyzed the specific Full-Time Equivalent (FTE) capacity dedicated to the daily management of internal reporting systems.

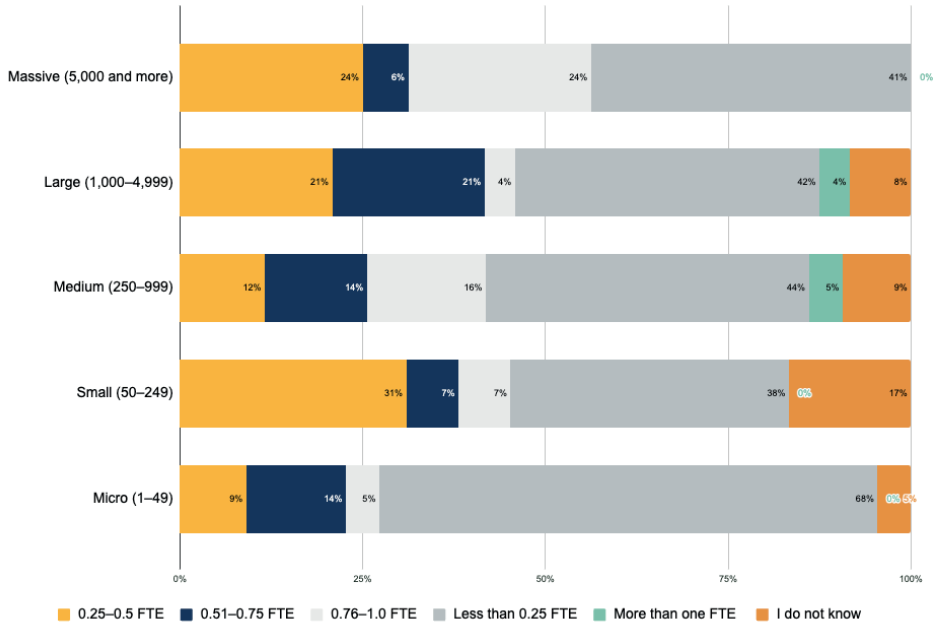
What is the total full-time equivalent dedicated in your organization for the daily operation and management of the internal reporting system?



While the required level of human resources naturally varies based on factors such as organizational size and the complexity of its operations, the data paints a concerning picture of possible under-resourcing. Specifically, 44.7% of organizations dedicate less than a quarter of a full-time position (0.25 FTE) to the Internal Reporting System. This suggests that for nearly half of the respondents, whistleblowing management is viewed as a minor administrative task rather than a professional function, leaving staff with fewer than 10 hours a week to manage reports, maintain security, and conduct investigations.

At the other end of the spectrum, only 13.3% (20) of organizations dedicate 0.76 FTE or more to the role. This suggests that specialized persons responsible for receiving and handling reports remain a rarity. However, aggregate FTE figures provide only a partial view of the landscape. To understand human resources allocated towards this activity we cross-referenced these resources with organizational size.

FTE by Organization Size



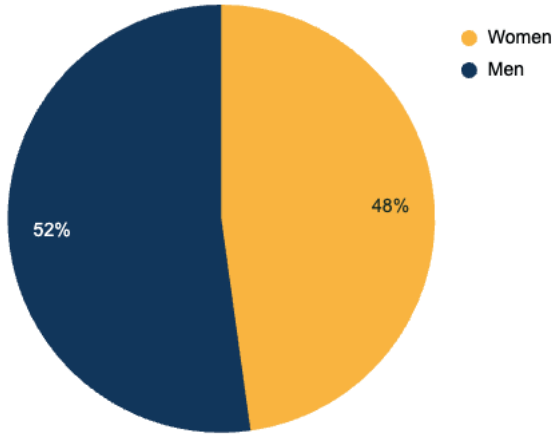
The cross-tabulation of organization size against FTE allocation reveals that while it is expected that micro organizations (1-49 employees) operate with minimal overhead (reflected in 68% of them dedicating less than 0.25 FTE to the task), assumption that resources would scale linearly with employee count is incorrect. Resource allocation remains stagnant regardless of organization size.

Surprisingly, the reliance on minimal staffing (less than 0.25 FTE) effectively flatlines across Medium (44%), Large (42%), and Massive (41%) organizations. This implies that a company with 5,000+ employees is often dedicating the same amount of time to whistleblowing management as a company of 250 employees.

3.4.2. Staffing and Gender Balance

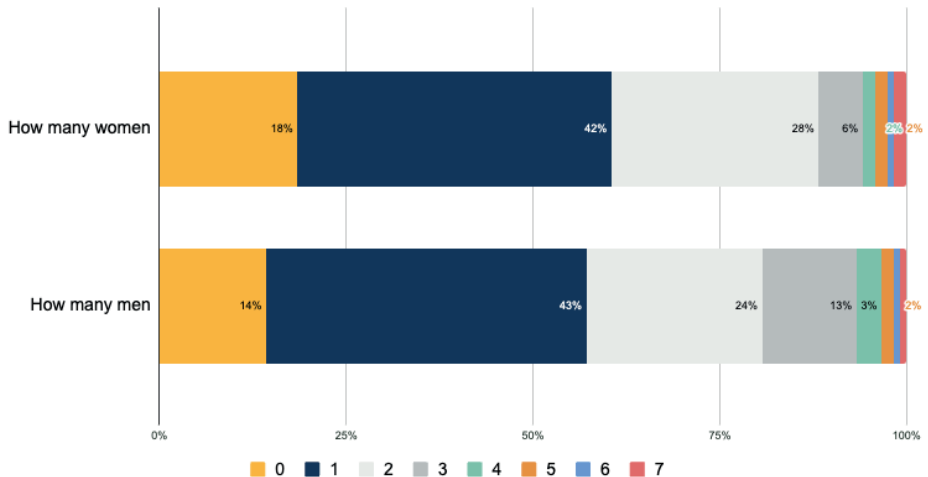
Data regarding the gender and number of responsible persons excludes the 21% of respondents who indicated they did not know how many people handle reports. This significant gap suggests that a portion of the survey respondents were not the actual workers responsible for the agenda, or simply declined to share this information for other reasons.

Gender of Designated Persons



When analyzing the gender distribution of the persons responsible for receiving and handling reports, the data shows a remarkably balanced workforce, dispelling the notion that this role is dominated by a single gender.

How many people are responsible for receiving and subsequently handling notifications?



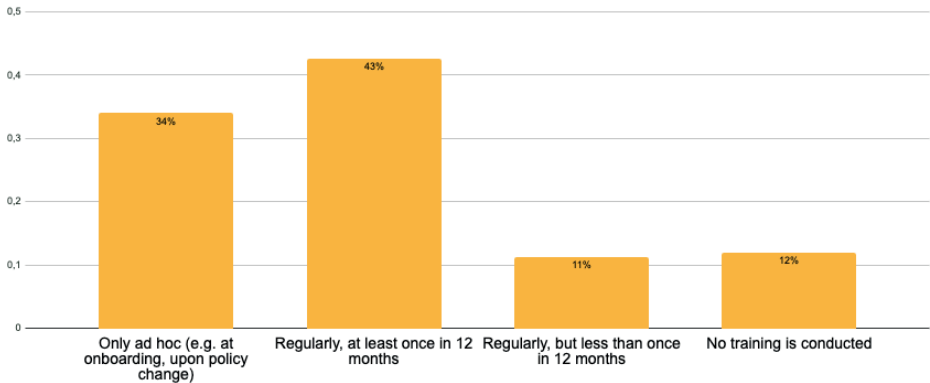
Data further show that 14% of organizations have zero men involved and 18% of organizations have zero women involved. In 39 organizations (representing 31.5% of those that specified gender ratios), the whistleblower has no choice regarding the gender of the recipient, potentially creating a barrier to reporting for sensitive issues. The presence of both men and women in the reporting structure is a best practice as whistleblowers reporting sensitive issues (e.g., sexual harassment or gender-based discrimination) often feel more comfortable disclosing to a specific gender.

Moreover, 25 organizations rely on a single individual to manage the internal reporting system. This creates a risk of not being able to acknowledge receipt of the report (or meet other time-strained obligations) due to illness or vacation of this single person.

3.4.3. Training Frequency for Persons Responsible for IRS

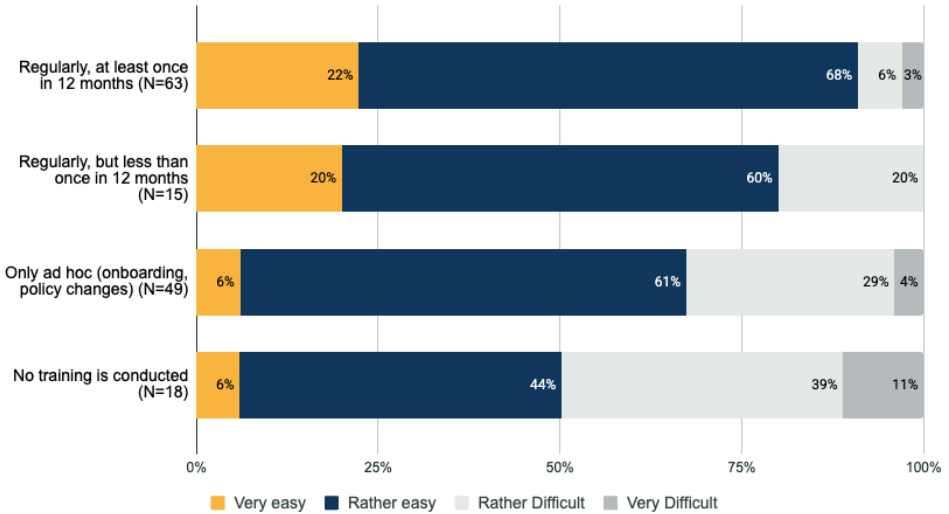
The efficacy of an Internal Reporting System relies on the capability of the persons responsible for the IRS to interpret complex legal frameworks and manage sensitive investigations. Therefore, their continuous professional development in whistleblower protection is essential.

How often does your organization train persons responsible for the operation of the internal reporting system?



The data indicates a slightly higher prioritization of specialists compared to general staff, with 43% of organizations ensuring regular training at least once every 12 months. However, a significant competency gap persists for the remaining majority. 34% of organizations rely solely on ad-hoc training which may leave persons responsible for the IRS management ill-prepared especially in a young field of whistleblower protection. Most alarmingly, 12% of organizations admit to conducting no training whatsoever for their responsible persons, creating a high-risk environment for both the organization and the whistleblower.

Correlation of Training Frequency and Legal Assessment Difficulty



The data confirms a robust positive correlation between the frequency of training and the confidence of designated persons in assessing the legal scope of reports. Among responsible persons who receive training at least once every 12 months, 90.5% report that assessing whether a report falls under the material scope of the Directive is „Easy“ or „Very Easy.“ This group demonstrates the highest level of operational capability, with 22.2% describing the task as „Very Easy.“

As training frequency decreases, so does legal confidence. For those trained only upon onboarding or policy changes, the confidence rate drops to 67.3% („Easy“ or „Very Easy“). In organizations where no training is conducted the same metric falls to exactly 50%.

The impact of regular education is most visible at the highest level of competence. Designated persons with annual training are nearly 4 times more likely to find legal assessments „Very Easy“ (22.2%) compared to those with no training (5.6%).

A similar logic applies to the relationship between regular training and the depth of whistleblower engagement. Designated persons who receive training at least once a year are significantly more likely to discuss follow-up measures with whistleblowers both before and after they are realized.

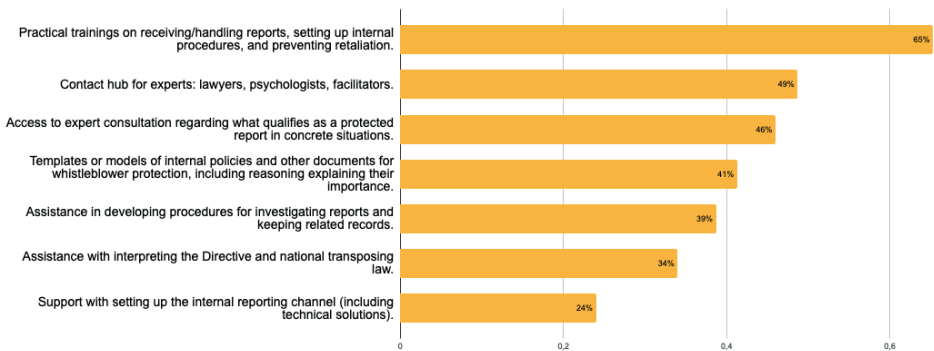
Among those trained annually, 42.2% (27 out of 64) engage in this dialogue. In stark contrast, only 5.6% (1 out of 18) of responsible persons with no training experience do the same. This suggests that training does not just improve legal compliance but it fundamentally shifts the professional's approach from a passive role to an active, communicative one.

3.5. Requested Support and Country-Specific Perspective

3.5.1. Requested Support

At the end of the questionnaire we asked respondents directly on which forms of support they would welcome to have the possibility to access for developing their internal reporting system.

Form of Support



Note: Based on 150 respondents in the source dataset; respondents could select multiple options.

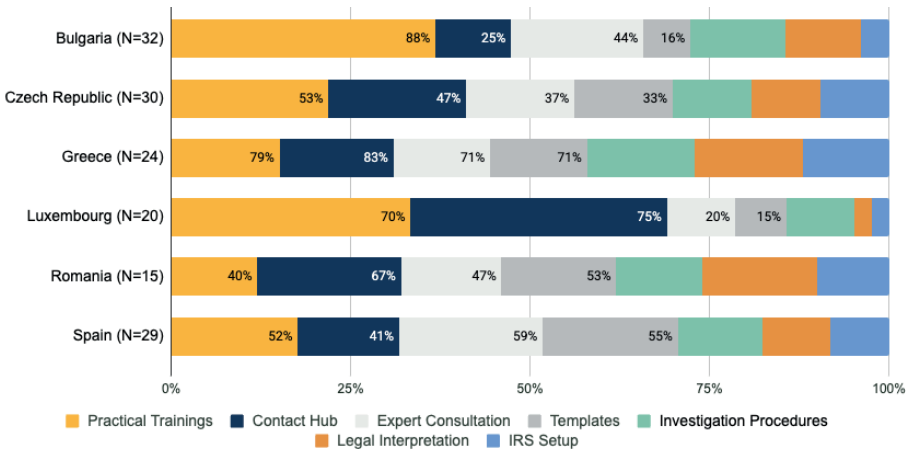
The data identifies practical competency as the primary deficit in the current landscape, with 65% of organizations prioritizing practical training on receiving and handling reports above all other forms of support. Beyond training, the results highlight a critical need for an external safety net, as nearly half of the respondents expressed a desire for real-time consultation regarding specific cases (46%) or access to an expert contact hub for lawyers and psychologists.

There is also a robust demand for best-practice templates (41%). These resources can either modernize internal rules or help to structure the communication of follow-up measures. This drive for operational consistency likely explains why the demand for assistance in developing investigation procedures tracks closely at 39%, confirming that organizations are seeking a standardized process to guide their actions.

3.5.2. Country-Specific Perspective

The country-specific data reveals that the challenges of the Directive are not uniform across the EU. Respondents in Greece showed the highest overall intensity of demand, with nearly 80% of organizations requesting assistance across almost every category, including training, expert hubs, investigation procedures, and legal interpretation. This pervasive need suggests a systemic demand for capacity building, where organizations feel under-equipped at every aspect of IRS management and whistleblower support.

Desired forms of Support by Country



In contrast, Bulgarian organizations demonstrate a targeted focus. Their overwhelming demand for practical training (87.5%) dominates, while interest in aid with infrastructure like IRS setup (9.4%) or document templates (15.6%) is minimal.

In Spain the desire for ad hoc expert consultations regarding specific protected reports (58.6%) surpasses the demand for general practical training. This suggests a shift in focus from learning general procedures to solving complex, case-specific legal cases. Meanwhile, both Luxembourg and Romania show a very strong preference for an expert contact hub (75.0% and 66.7% respectively), yet the context differs. Luxembourg shows negligible interest in templates (15%) or legal interpretation (5%), implying a confident internal legal structure that simply identifies the need for whistleblowers' potential need for expert aid as the expert hub may serve both the designated person and the whistleblower. Romania, conversely, pairs this demand for experts with a continued need for legal interpretation (53.3%), pointing to a landscape where legal clarity is still being established alongside the need for expert networks. The Czech Republic remains the most balanced environment, with a moderate demand spread evenly across all categories.

Analysis of legal assessment difficulty to assess whether a report falls under the scope of the Directive or national whistleblower protection law across the surveyed countries reveals that organizations in Romania report the highest level of struggle, with 33.3% of respondents finding it difficult to determine if a report falls within the legal scope of the Directive or national law. Greece follows closely at 29.2%, while Spain and the Czech Republic occupy a middle tier where 27.6% and 26.7% of organizations, respectively, find assessments rather or very difficult. Conversely, legal confidence is highest in Luxembourg and Bulgaria, where only 10.0% and 9.4% of organizations reported difficulty in assessing the legal standing of notifications. Drawing on these findings, the following table summarizes the perceived organizational needs and priority skills across each surveyed country:

Support Category	Bulgaria	Czechia	Greece	Luxembourg	Romania	Spain
Practical trainings on receiving/handling reports, setting up procedures.	High (88%)	Medium (53%)	High (79%)	High (70%)	Medium (40%)	Medium (52%)
Contact hub for experts: lawyers, psychologists, facilitators.	Medium (25%)	Medium (47%)	High (83%)	High (75%)	High (67%)	Medium (41%)
Access to expert consultation regarding what qualifies as a protected report.	Medium (44%)	Medium (37%)	High (71%)	Low (20%)	Medium (47%)	High (59%)
Templates or models of internal policies and other documents.	Low (16%)	Medium (33%)	High (71%)	Low (15%)	Medium (53%)	Medium (55%)
Assistance in developing procedures for investigating reports and keeping related records.	Medium (31%)	Medium (27%)	High (79%)	Low (20%)	Medium (40%)	Medium (35%)
Assistance with interpreting the Directive and national transposing law.	Medium (25%)	Low (23%)	High (79%)	Low (5%)	Medium (53%)*	Medium (28%)
Support with setting up the internal reporting channel (including technical solutions).	Low (9%)	Low (23%)	High (63%)	Low (5%)	Medium (33%)	Low (24%)

4. Conclusion

Despite high levels of formal legal compliance, the internal reporting landscape in the six selected EU member states remains fragmented. The analysis indicates that the organizations currently lack the operational maturity required to truly protect whistleblowers. While the organizations usually follow the legal provisions, they have largely not yet been able to integrate a truly functional, protective and supportive whistleblower protection environment.

This disconnect is apparent in the visibility and accessibility of the internal reporting system (IRS). While the majority of organizations meet the formal requirement of publishing information on a public website, a significant disparity exists between this external visibility and internal embedding: only 17.3% of organizations include IRS references in employment contracts, and nearly 60% of regular employees receive either no training or only through an one-and-done approach. This means that for many employees, the reporting system is theoretically available but practically invisible in their daily professional lives.

While a maturing segment of organizations (22.67%) has implemented two-way anonymous communication to prioritize the content of a report over the reporter's identity, a substantial minority of organizations (26%) refuse to accept anonymous reports entirely and another 13% of organizations condition investigation on sufficient supporting information while not enabling two-way communication. This creates a space where valid concerns are stalled or rejected because the system demands evidence that cannot be safely provided without a secure, identity-blind channel.

The data also reveals that at least 17% of organizations struggle to consistently acknowledge the receipt of reports within the mandatory 7-day window. This inability to meet the very first legal deadline in the whistleblowing process signals a profound lack of procedure and a lack of capacity. When organizations fail at this initial stage, it creates an immediate breakdown in trust, suggesting to the whistleblower that the system is either unmonitored, under-resourced, or indifferent to their disclosure.

Furthermore, we analyzed a significant gap in whistleblower consultation where organizations tend to treat whistleblowers as passive data sources rather than partners. While 17% of organizations are willing to review follow-up measures retrospectively, only 11% discuss follow-up actions with whistleblowers before their implementation. Importantly, organizations also prioritize post-damage complaints over active prevention. Despite 36% having procedures for lodging retaliation complaints, only 20% monitor for retaliation risks proactively, and a mere 14.7% train managers in retaliation prevention, meaning the system is better equipped to process damage than to prevent it.

Underlying many of these issues are gaps in resource allocation and professionalization. 45% of respondents claim the organization allocates 0.25 full-time equivalent or less for the management of internal reporting systems. Additionally, nearly one-third of organizations (31.5%) offer no gender choice for reporting sensitive issues, and 25 of 150 organizations rely on a single

individual to manage the IRS, creating a single point of failure where illness or leave can cause immediate non-compliance with the Directive. Finally, the analysis reveals a significant demand for expertise building and external support. A substantial majority of organizations (65%) express a need for practical training on receiving and handling reports, setting up internal procedures, and preventing retaliation.



Whistleblower
Empowerment
& Support Initiative



Co-funded by
the European Union



Project co-funded by the European Union through the European Commission - Citizens, Equality, Rights and Values Programme (CERV)

