

How to Build a Worldclass Whistleblower Program



CPAs & ADVISORS

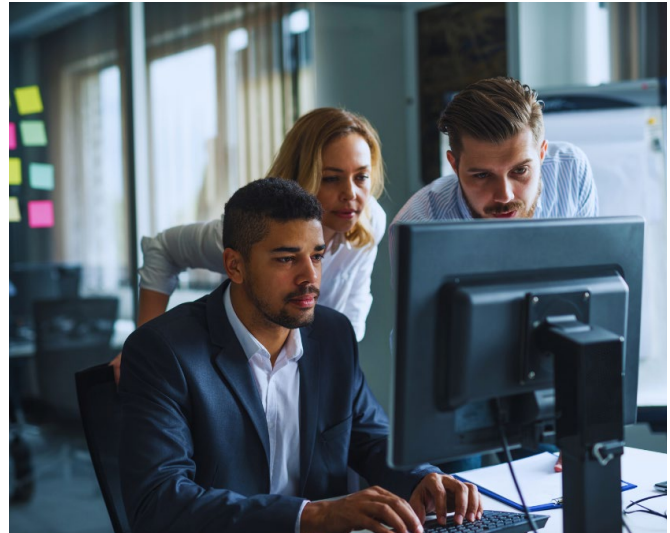
Contact Us

Melissa Musser
CPA, CIA, CITP, CISA
Partner and Director,
Risk & Advisory Services
mmusser@grfcpa.com

**Mac Lillard, CPA/ABV/CITP,
CIA, CFE, CISA/CRISC**
Senior Manager,
Risk & Advisory Services
mlillard@grfcpa.com

Index

• Introduction	2
• Governance and Organizational Culture	8
• The Whistleblower Process	15
• Continuous Monitoring and Improvement	28
• Closing Thoughts	31
• GRF Can Help	32
• Resources and References	33
• Glossary of Key Terms	34
• Appendices	36



Introduction

Whistleblower programs are essential elements of effective risk and governance frameworks, as they enable organizations to identify and address potential fraud and misconduct before they escalate into costly and damaging crises.

By providing a safe and confidential channel for employees and other stakeholders to report concerns, whistleblower programs enhance organizational transparency, accountability, and integrity.

Statistics from the Association of Certified Fraud Examiners (ACFE) *Report to the Nations* support this claim, revealing the vital role whistleblower programs play in detecting and preventing fraudulent activities within organizations. Organizations with effective whistleblower hotlines detected fraud more quickly and experienced lower median losses compared to those without such programs. Tips were the most common initial detection method, accounting for 43% of cases, with employees being the source of over half of these tips, and vendors/customers accounting for another third. Moreover, organizations that supported anti-fraud mechanisms such as whistleblower programs experienced a 50% reduction in fraud losses and duration. These findings demonstrate the tangible benefits of fostering a culture where employees feel



safe and encouraged to report suspicious activities. By leveraging the insights gained from whistleblowers, companies can not only detect and address fraud more efficiently, but can also implement preventive measures that strengthen overall organizational resilience.

The Committee of Sponsoring Organizations (COSO) and ACFE's *Fraud Risk Management Guide, Second Edition* emphasizes the necessity of a whistleblower program as part of a comprehensive fraud risk management strategy. It highlights that an effective whistleblower mechanism can serve as an early warning system, allowing organizations to detect and address potential fraud risks before they escalate.

The Institute of Internal Auditors (IIA) 3 Lines Model further underscores the importance of integrating governance, management, and assurance roles to foster a culture of accountability. A well-designed whistleblower program aligns with this model by providing a secure and confidential mechanism for employees and stakeholders to report unethical behavior, thereby enhancing the organization's overall risk management framework.

Given the complex and dynamic corporate environment, establishing an effective whistleblower program is not merely a compliance requirement but the cornerstone of ethical governance and organizational integrity. Such programs empower employees to report misconduct, fraud, and other unethical behaviors without fear of retaliation, thereby fostering a culture of transparency and accountability. An effective whistleblower program not only helps in early detection and mitigation of risks but also enhances the trust of stakeholders, including





employees, customers, investors, and regulators. By ensuring that concerns are addressed promptly and appropriately, organizations can safeguard their reputation, maintain legal compliance, and promote a positive, ethical workplace culture.

This whitepaper delves into the critical components and best practices for developing a robust whistleblower program, emphasizing its role in reinforcing ethical standards and protecting organizational value. We will explore the key elements of building an effective whistleblower program, drawing on best practices and guidance from the COSO/ACFE *Fraud Risk Management Guide*, the IIA's *3 Lines Model and Global Internal Audit Standards*, and other leading best practice guidance. The goal is to provide a practical roadmap for organizations seeking to enhance their governance and risk management practices through the implementation of a whistleblower program.



Anti-Fraud Program vs Whistleblower Program

The whistleblower program plays a critical role in the organization's comprehensive anti-fraud program and it is important to understand the similarities and differences between these groups.

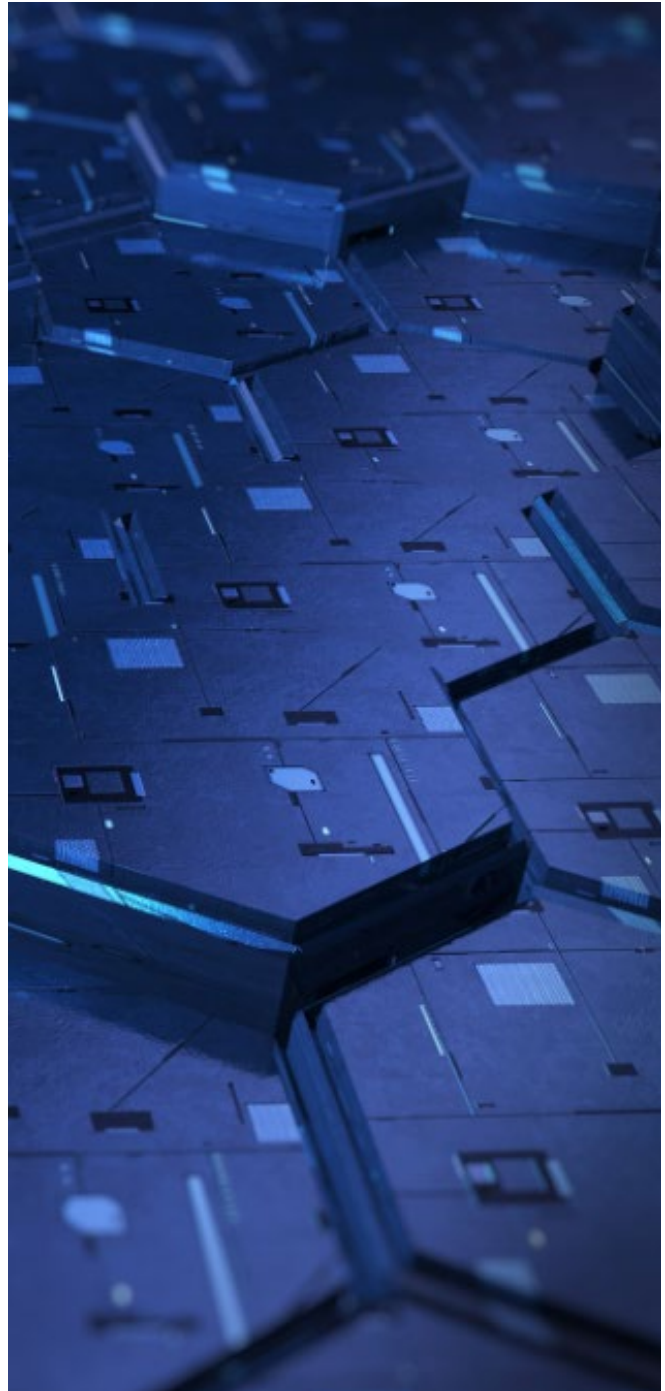
	 Anti-Fraud Program	 Whistleblower Program
Purpose	The anti-fraud program is a broader initiative that encompasses policies, procedures, and controls designed to prevent, detect, and respond to fraud within an organization.	The whistleblower program provides a mechanism for employees, vendors, customers, and other stakeholders to report unethical behavior, including fraud, anonymously or confidentially, without fear of retaliation.
Scope	It includes multiple components like internal controls, fraud risk assessments, fraud prevention training, internal audits, and fraud detection mechanisms, such as data analytics.	It primarily focuses on the detection of fraud by encouraging individuals to report suspicious behavior, however, employee misconduct or other behavioral complaints are commonly received through the whistleblower program.
Key Elements	<ol style="list-style-type: none"> 1. Fraud Risk Management: Identifies and assesses fraud risks across the organization. 2. Internal Controls: Implements, oversees, and/or audits controls to prevent and detect fraud. 3. Monitoring and Reporting: Includes regular monitoring of controls, fraud detection activities, and reporting mechanisms, including the whistleblower program. 	<ol style="list-style-type: none"> 1. Reporting Mechanisms: Hotline, email, or web-based platforms for reporting. 2. Confidentiality and Anonymity: Ensures that whistleblowers can report issues without fear of retaliation. 3. Policies and Procedures: Guidelines for handling whistleblower reports, conducting investigations, and protecting whistleblowers.
Response Plans	Outlines how the organization will respond to detected fraud, including investigations and corrective actions.	Outlines how the organization will respond to the specific allegations and findings related to whistleblower complaints received.
Oversight and Responsibility	<ol style="list-style-type: none"> 1. Usually overseen by a combination of internal audit, compliance, and risk management functions. 2. Specific responsibilities may be divided among the Chief Financial Officer (CFO), Chief Audit Executive (CAE), Chief Compliance Officer (CCO), and other senior management. 3. The board of directors, particularly the audit committee, also plays a critical role in overseeing the anti-fraud program to ensure it is comprehensive and effective. 	<ol style="list-style-type: none"> 1. Typically overseen by a dedicated compliance officer, ethics officer, or a whistleblower program manager. 2. Reports are often directed to an independent party, such as an internal audit function or a third-party provider, to ensure confidentiality and impartiality. 3. The audit committee or board of directors often provides oversight, especially in cases involving senior management.



Best Practices for Integration

While the whistleblower program and the anti-fraud program have distinct roles, they are interdependent and must be effectively integrated to support an organization's overall fraud risk management strategy. The oversight structure typically involves different individuals to maintain objectivity, but they must work collaboratively to achieve a cohesive and effective anti-fraud environment. Best practices to consider in defining your anti-fraud and whistleblower programs include:

- **Independence and Objectivity:** Ensure that the individuals overseeing the whistleblower program are independent from those responsible for operational management to avoid conflicts of interest.
- **Clear Roles and Responsibilities:** Define clear roles and responsibilities for managing the whistleblower and anti-fraud programs to ensure effective implementation.
- **Staffing and Structure:** Assess the needs of the programs and the current capabilities to ensure the programs are staffed with the necessary skills, knowledge and expertise, and that the appropriate reporting lines are in place.



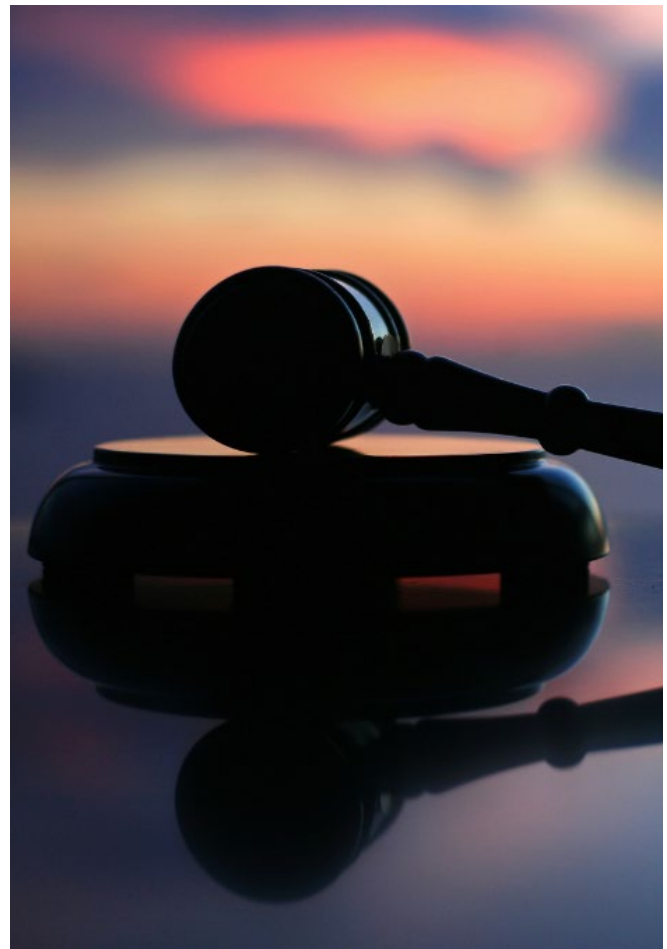
Legal and Compliance Considerations

Depending on your organization's size and structure, you may be subject to certain legal and regulatory requirements when running a whistleblower program, such as:

- **[Sarbanes-Oxley Act \(SOX\), Section 301\(m\)\(1\)\(4\)\(a-b\)](#)**: For publicly traded companies, SOX mandates mechanisms for confidential and anonymous submission of concerns regarding questionable accounting or auditing matters.
- **[Dodd-Frank Act](#)**: This law provides additional protections and incentives for whistleblowers in the financial sector.
- **[European Union Whistleblower Directive](#)**: This directive requires anonymous reporting channel for whistleblowers, identity protection, reporting deadlines, and anti-retaliation protocol.
- **[B-Corp Certification](#)**: While not a requirement, this certification is given to companies that meet high standards of environmental, social, and governance (ESG) by demonstrating a commitment to accountability and transparency. Whistleblower programs help address specific questions for certification related to anti-corruption mechanisms.

The information contained in this white paper is meant to be universal in application and not tailored to a specific legal or regulatory framework. The processes and information contained on the subsequent pages draw on best practices from a

variety of resources, including publications from COSO, the IIA, the ACFE, the Society for Human Resources Management (SHRM), among others, and may be used as a guide by practitioners seeking to implement or improve a whistleblower program. The development of anti-fraud and whistleblower programs should engage all relevant stakeholders within the organization, including legal, compliance, insurance, etc., and should be reviewed against applicable requirements to assess the level of compliance.



Business Case for a Whistleblower Program

A robust whistleblower program is a crucial component of a company's internal controls and risk management strategy, as it serves to detect and mitigate fraud before significant financial and reputational damage occurs. A well-implemented whistleblower program acts as an early warning system, identifying potential risks and misconduct before they escalate into major issues, which could result in legal penalties, regulatory scrutiny, or reputational harm. The cost of fraud often far exceeds the investment required to operate a whistleblower program, making it a cost-effective measure for safeguarding organizational resources. Implementing such a program also reinforces a company's zero-tolerance stance on unethical behavior and demonstrates a commitment to strong governance, aligning with environmental, social, and governance (ESG) principles. Additionally, it communicates a clear message from leadership that ethical conduct is a priority, fostering a culture of accountability and transparency throughout the organization.

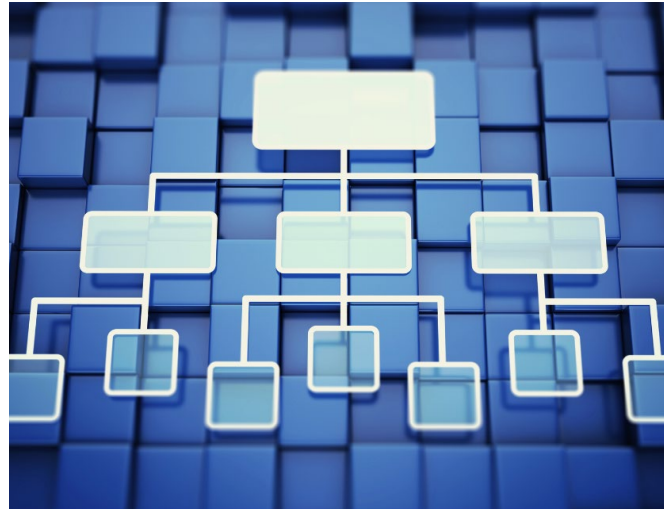
A whistleblower program can enhance relationships with key stakeholders—such as investors, customers, and regulators—by demonstrating a proactive approach to corporate governance and risk management. In industries where compliance is critical, it also helps ensure adherence to regulatory requirements, reducing the likelihood of fines or sanctions. These points help illustrate how a whistleblower program strengthens overall operational resilience while contributing to long-term business sustainability.



Governance and Organizational Culture

The success of a whistleblower program is deeply rooted in the organization's culture, where the tone at the top plays a pivotal role. Leadership must demonstrate a commitment to ethical practices, fostering an environment where integrity is prioritized and where employees feel empowered to speak up without fear of retaliation. Open and transparent communication is essential, as it builds trust and encourages employees to report concerns, knowing their voices will be heard and taken seriously. A strong non-retaliation policy further reinforces this trust, ensuring that those who come forward are protected and that the organization is genuinely committed to addressing and correcting issues. Without these foundational elements, a whistleblower program is unlikely to achieve its intended purpose, as fear and skepticism can easily undermine its effectiveness. According to the *Fraud Risk Management Guide*, Second Edition, "the Board of Directors and top management have the responsibility for managing fraud risk." However, for the program to be effective, all employees should be trained on the process and understand their role. It's important to note that the structure of the whistleblower program will be unique to each organization and should be representative of the overall organizational structure, size, and risk profile of the organization.

As a first step, define the roles of the Board of Directors and senior management. The Board is responsible for oversight of the whistleblower program. The Board provides guidance, review/



approval of the underlying fraud response plan and supporting policies, and may potentially be directly involved in certain aspects of the program. Senior management is responsible for administration of the plan, development of policies for Board approval, and informing the Board of whistleblower allegations, investigation results, and other relevant information. The underlying program documentation should provide the Board with the authority to conduct investigations independent of senior management's approval.

Identify a champion and delegate the appropriate resources to setting up the structure, process, and reporting lines. The champion should be a senior-level employee who supports a strong tone at the top and should have the skills, knowledge, and expertise to properly oversee the program. The whistleblower program will ideally be a part of the organization's overall anti-fraud program and will have dedicated resources through finance, information technology, internal audit, legal, and compliance.



The *Pulse of Internal Audit* issued by the Institute of Internal Auditors says that Chief Audit Executives (CAEs) are responsible for investigations, while the *Executive Perspectives on Top Risks Report* states that the Chief Financial Officer (CFO) and Chief Risk Officer (CRO) are responsible for fraud prevention. If your organization is larger and has one individual at each of these roles, define the level of communication between these groups and how are fraud prevention measures influenced by investigations (and vice versa). In smaller organizations, these roles may not exist or are being filled by one individual who wears multiple “hats” – in this case, ensure adequate segregation of duties and proper resource allocation with limited capacity. The champion is responsible for assessing the expected level of effort to support the whistleblower program on an annual basis, budget accordingly, and request resources for management’s approval, as necessary.

The leadership of whistleblower programs varies across industries and organizational structures. Matt Kelly, CEO and Founder of Radical Compliance and a long-time observer of corporate compliance, has noted that in many corporate environments, the Chief Compliance Officer (CCO) typically oversees the program, with support from Human Resources, Internal Audit, and Legal. This structure aligns with regulatory expectations and corporate governance frameworks emphasizing compliance-driven ethics programs.

In privately held organizations, whistleblower program ownership varies widely. Larger private companies with established compliance functions may follow a corporate model with the CCO or General Counsel



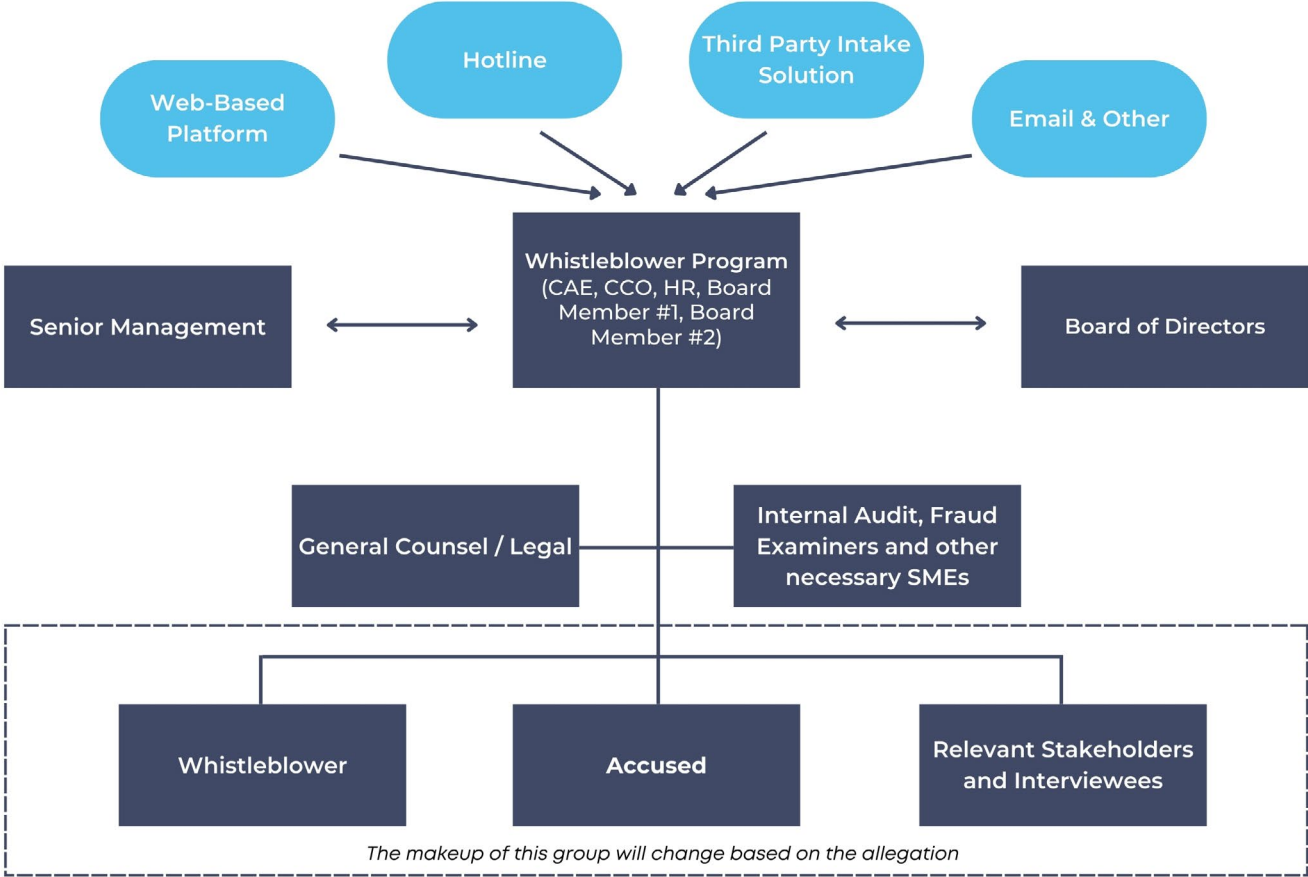
leading the program. In smaller or family-owned businesses, whistleblower programs may be managed by Human Resources (HR), legal counsel, or an independent risk function, though they often face challenges in maintaining whistleblower anonymity and independent oversight.

In nonprofits, including international NGOs (INGOs), the Chief Audit Executive (CAE) or a designated ethics officer often leads the whistleblower program, given their focus on governance, risk management, and fraud prevention. In these settings, HR, general counsel, and other departments play supporting roles to ensure effective intake, investigation, and resolution of whistleblower reports.

In associations and membership organizations, whistleblower program leadership varies but often falls under Legal, HR, or a dedicated Ethics & Compliance Officer, sometimes with Internal Audit involvement. Since these organizations serve members rather than external stakeholders, they may take a more corporate approach to compliance and risk management.



The graphic below depicts an example governance structure in which the whistleblower program is championed by the Chief Audit Executive and supported by the Chief Compliance Officer, HR and members of the Board. General Counsel / Legal serves as support and guidance throughout the process, along with other necessary subject matter experts such as Certified Fraud Examiners and Certified Internal Auditors. The program is reliant on the whistleblower, the accused, and other relevant stakeholders to adequately participate in investigations. The Board receives information from the whistleblower program – including details of allegations received, results of investigations, and action items – on a periodic basis (i.e., monthly, quarterly). The champion will also collaborate with senior management on an ongoing basis for the purposes of determining resource allocation, communication of program activities, and in performing investigations.



In the ACFE's *Building a Best-in-Class Whistleblower Hotline Program*, a US-based Internal Auditor described their process:

“We have a working group that consists of Human Resources, Security, Legal, Compliance and Internal Audit. This group meets regularly to see what items are being reported in the hotline, distributes the future investigation to the proper group, reviews the results and meets with the CEO quarterly to review the statistics of the program. The CEO provides great tone at the top leadership on this program. All this is reported to the Audit Committee on a quarterly basis.”

In this example, the champion or administrative leader (in this case, the CEO) is a member of senior management, is supported by other functions within the organization, and reports regularly to the Board of Directors.



Laying the Groundwork

Performing a baseline review of existing policies is a good first step in setting up a whistleblower program. This process involves assessing current policies to identify gaps, inconsistencies, or areas that may not fully support a robust whistleblower framework. As stated in *Managing the Business Risk of Fraud: A Practical Guide*, “documentation should not only articulate the organization’s zero tolerance for fraud, it should also establish the expectation that suspected fraud must be reported immediately and provide the means to do so.” By understanding the existing landscape, organizations can ensure that the new program is built on a solid foundation that aligns with best practices and legal requirements.

Fraud Risk Management Program Document:

The fraud risk management program document serves as the foundational framework for identifying, mitigating, and responding to fraud risks within an organization. It outlines the organization’s commitment to ethical practices, defines key roles and responsibilities, and establishes protocols for monitoring, investigating, and reporting fraud-related activities. This document will outline the purpose and authority of the Whistleblower Program. Specifically, it should include the following information related to the authority of the whistleblower program:

- Identify members of senior management and the Board of Directors who are responsible for administration and oversight of the program.
- Grant the Board of Directors authority to conduct investigations into the organization’s operations, independent of senior management’s approval.



Whistleblower Policy: The whistleblower policy outlines the procedures for reporting unethical or illegal activities within the organization. It ensures that employees know how and where to report concerns, and that their reports will be taken seriously and addressed appropriately. This may be the first place a potential whistleblower looks for guidance, so it should be clear and comprehensive.

Code of Conduct: The code of conduct defines the ethical principles and behavioral standards expected of all employees. It serves as the foundation for the whistleblower program by establishing a clear framework for identifying and reporting misconduct.

Non-Retaliation - Protection for Whistleblowers: Ensuring protection for individuals who report in good faith is crucial for encouraging participation and maintaining trust in the program. This includes:

- **Confidentiality:** Protecting the identity of the whistleblower to the fullest extent possible.
- **Non-Retaliation Policy:** Enforcing strict policies against retaliation and providing support to whistleblowers.
- **Follow-Up:** Keeping the whistleblower informed about the progress and outcome of the investigation, when appropriate.

Conflict-of-Interest: The conflict-of-interest policy prevents situations where personal interests could compromise an employee's ability to act in the best interests of the organization. It supports the whistleblower program by ensuring that potential conflicts are identified and managed appropriately to allow for independent and unbiased review of the case.

Information Security Policy: The information security policy ensures that all whistleblower reports and related data are handled with the highest level of confidentiality. This policy protects sensitive information from unauthorized access to maintain the integrity of the program. Helpful resources in developing an information security policy include the [SANS Institute webpage](#) and the [ISACA Policy Toolkit](#).

Investigation Policy: The whistleblower investigation policy outlines the process for thoroughly and impartially investigating reports of misconduct made through the program. It ensures that all allegations are reviewed promptly and that investigations are conducted with fairness, confidentiality, and respect for all parties involved. The policy also establishes clear responsibilities for those conducting the investigation and sets expectations for how findings will be documented, communicated, and acted upon, ensuring that the organization addresses issues effectively and maintains trust in the whistleblower program. The policy will also include information on when to inform relevant parties, such as legal counsel, insurance carrier, public relations team, regulatory bodies, etc.



Case Management

Case management is a critical element to define clearly and thoroughly. It will guide how the organization manages individual allegations, aggregates data and information, standardizes the process across departments, offices, regions, etc., and supports decisions made and actions taken based on the results of the assessment. *The Fraud Risk Management Guide, Second Edition* advises that “a single case management system is the optimum method of logging and consolidating all reports and the follow up actions (regardless of whether they surface through the whistleblower system or other channels).” Effective case management is essential in the whistleblower process, as it ensures that reports are tracked, investigated, and resolved in a systematic and efficient manner.

Web-Based Platforms

Web-based platforms offer robust solutions for end-to-end case management, providing a central repository where all relevant documentation, communication, and evidence can be securely stored and accessed. These platforms streamline the workflow by allowing for the assignment and monitoring of investigation tasks, ensuring that responsibilities are clearly defined, and deadlines are met. Benefits include:

Automated notifications and progress tracking:

Web-based systems enhance transparency and accountability throughout the investigation, enabling organizations to respond to issues more swiftly and effectively. Notifications can be set to ensure

compliance with reporting deadlines under relevant requirements.

Customization: Your organization can categorize allegations by location (i.e., department, office, region), type of allegation (i.e., employee misconduct, corruption, fraud, embezzlement), and other data points. This allows the organization to set up multiple teams to respond quickly as allegations are received.

For example, you can have a team of legal and forensic experts designated to receive and investigate allegations of fraud/corruption/embezzlement in Africa, while having a separate team of legal and forensic experts designated to receive and investigate allegations of fraud/corruption/embezzlement in the United States, or employee misconduct in Asia, or bribery/kickbacks in Europe. Each team would have limited access rights to restrict access to only relevant documentation and information for the allegations to which they are assigned.

Data analytics: The organization can track data regarding volume of allegations, time of year, individuals involved, response time, resolution time, etc. This data can be used when assessing the organization’s process, controls, and effectiveness at macro and micro levels.

Excel and Other Mechanisms

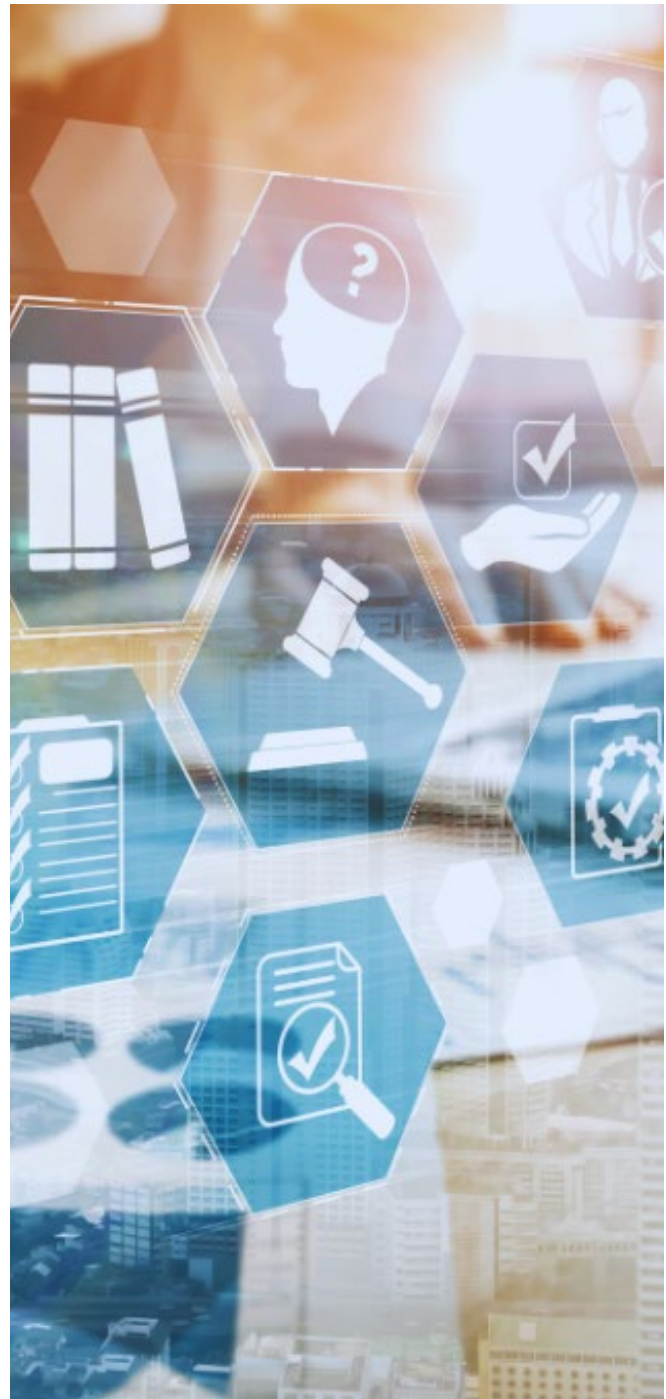
Even without a web-based platform, organizations can still achieve effective case management using tools like Excel. Although more manual, Excel can be used to create a central database for tracking cases, documenting evidence, and managing the workflow



of tasks. Organizations can replicate many of the functionalities of a more sophisticated system by carefully designing spreadsheets to capture key details and using formulas to set deadlines and track progress. This approach may require more effort and vigilance, but it can still provide a structured and organized way to manage whistleblower cases, ensuring that nothing falls through the cracks.

Access Management

Setting up information technology access controls on data and work products associated with a whistleblower investigation is critical to maintaining confidentiality, data integrity, and the overall credibility of the process. Sensitive information involved in such investigations, including witness statements, evidence, and reports, must be protected from unauthorized access to prevent tampering, leaks, or retaliation against whistleblowers. Effective access controls, such as role-based access, encryption, and multi-factor authentication, help ensure that only authorized personnel can access, modify, or disseminate investigation-related data. This not only safeguards the privacy and safety of all parties involved but also helps preserve the legal defensibility and objectivity of the investigation's findings. Without these controls, the organization risks reputational damage, potential legal liability, and a breakdown of trust in its internal controls and whistleblower protection mechanisms.



The Whistleblower Process

A well-defined whistleblower process is key for the success of the program, as it ensures that all reports are handled promptly, fairly, and consistently. Organizations can significantly reduce response times and improve overall efficiency by establishing a clear, step-by-step procedure for receiving allegations and conducting investigations. This pre-defined process also helps maintain objectivity, as it provides a standardized approach that minimizes the risk of bias or inconsistency. Moreover, an established process enhances the credibility of the program by demonstrating the organization's commitment to thoroughly addressing concerns raised by employees.



1 Intake

The intake process involves the initial receipt and logging of reports through the various reporting mechanisms and consolidating into the central repository. To ensure proper segregation of duties and maintain the integrity of the process, at least two individuals should have access to the whistleblower systems. This dual-access approach helps prevent any single person from having undue influence over the handling of reports, thereby reducing the risk of manipulation or oversight. Depending on the size of your organization and the volume of whistleblower allegations received, you may need to explore third party solutions to assist in the intake process. For example, Fortune 500 companies can receive upwards

of 1,000 allegations a year through the various whistleblower mechanisms, and reviewing and assessing each allegation would be an administrative burden. Third party providers assist the organization by standardizing the intake process through designing intake forms, crafting discovery questions, and creating risk-ranking methodology to systematically evaluate each allegation based on a consistent framework. Then, they can distribute allegations to relevant personnel at the organization to take next steps. They can also provide reporting mechanisms such as hotlines and web-based platforms to manage the process in one centralized system. These benefits help to streamline the process, reduce risk for the organization, and allow management to allocate resources to prioritize allegations.



COSO/ACFE notes that a “single case management system is the optimum method of logging and consolidating all reports and the follow-up actions.” There can be multiple channels for reporting, but all channels should be consolidated into a single repository that is strictly controlled to limit access based on principle of least privilege and encrypted to provide additional security. The most popular reporting mechanisms based on number of allegations received, as presented by the *ACFE Report to the Nations*, are below, listed from highest to lowest number of allegations received:

- Web-Based/online form
- Email
- Hotline
- Mailed letter/form
- Other, text message, fax

Capturing the intake information in a central repository can be accomplished in multiple ways depending on your organization’s risk tolerance and procedures. You can consolidate allegations in a central database or workbook, or set them up on a case-by-case basis and segregate them from one another to provide enhanced security. When using multiple reporting mechanisms, the investigation policy should define how the information is consolidated. For example, you may be entering data into a web-based platform from other formats (i.e., hotline, email, direct reporting), or exporting data from the platform into an excel spreadsheet or other mechanism to create an aggregate database with other whistleblower allegations.

See the following Excel-based templates that can be utilized if the organization does not leverage a web-based reporting platform.

- [COSO Fraud Risk Management Template](#)
- [Whistleblower Allegation Listing Template](#)
- [Whistleblower Investigation Detail Template](#)

See additional information in [Case Management section](#).



2 Preliminary Assessment

Review initial allegation and supporting materials to understand facts and circumstances, assess whether an investigation is necessary, and determine next steps. The investigation policy should assign responsibility to an individual, group of individuals, or a third party to perform the preliminary assessment and present findings to relevant stakeholders. It is important to note that not everything requires a formal investigation and based on the nature of the allegation, there may be a more appropriate course of action. In addition to formal investigations, allegations can be resolved via:

- a. **Informal Resolution or Mediation:** Engage in a dialogue between the parties involved to resolve the issue without a formal investigation. This can be particularly useful for minor disputes or misunderstandings.
- b. **Corrective Action:** If the allegation involves a clear and straightforward issue, the organization can take immediate corrective action to address the problem without further investigation.
- c. **Anonymous Feedback Channels:** Use anonymous reporting mechanisms to gather more information or clarify the whistleblower's concerns before deciding on the need for a formal investigation.
- d. **Policy Revision or Training:** If the allegation points to a broader issue with company policy or culture, consider revising policies or conducting targeted training sessions to address the concerns without a formal investigation.

Determining the appropriate intake process will be dependent upon your available resources and your expectations on the volume of allegations. We have provided a few alternatives based on different sized organizations to consider below:

- a. **Outsource Intake Process:** Large, multi-national, and/or public companies may choose to outsource the intake process. This involves engaging a third party to review the initial allegation submitted through a platform (typically web-based and/or hotline), perform an initial assessment based on defined criteria set by the organization, and route to the appropriate parties. Outsourcing offers several benefits: it standardizes the process so that all allegations are assessed using the same criteria by trained professionals, significantly reduces the administrative burden for management (especially in large organizations that may receive over 1,000 complaints annually), and allows the organization to focus on prioritizing complaints, leading to more efficient resource allocation and risk mitigation.
- b. **Whistleblower Committee:** For small-to-medium sized organizations, establish a Whistleblower Committee of 3-5¹ individuals who will be responsible for analyzing the allegation and voting as to whether it necessitates formal investigation. This committee should be diverse and may include representatives from HR, legal, compliance, executive leadership, and the Board. Consider designating backup committee members in case there are allegations involving members of senior management or the Board of Directors. Such cases may require



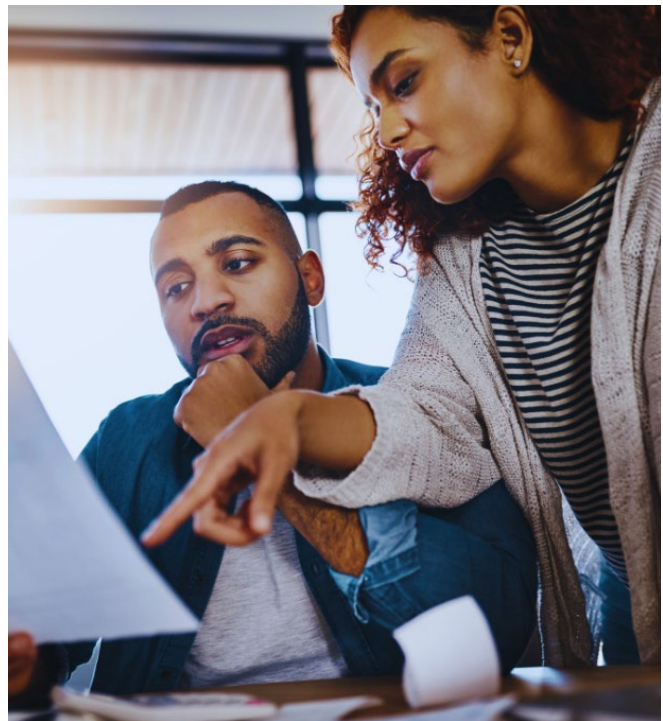
additional members of the Board, legal counsel, or independent third parties to take place in the initial assessment.

- c. **Champion of the Whistleblower Program:** For small organizations with limited capacity, the champion of the Whistleblower Program may be the sole individual responsible for the intake and preliminary assessment process. In these instances, it is even more important that this individual be someone of high moral character. It is also a best practice to identify at least one other individual who will have access to the whistleblower mechanism and case management system for oversight purposes.

Be sure to document the results of the preliminary assessment and communicate with the whistleblower to let them know next steps. Documenting the results is essential for creating a clear and organized record of the findings which justified management's response to an allegation. This documentation should include a summary of the allegation(s), steps taken during the preliminary assessment, the evidence reviewed, the severity and time sensitivity of the allegations/ investigation (if deemed necessary), the justification/ rationale for management's response, and actions to be taken. It ensures that the process is transparent and provides a reference point for the investigation team. Additionally, communicating with the whistleblower is an important step, as there are compliance requirements under certain frameworks such as the European Union Whistleblower Directive that require acknowledgement of the report within 7 days of receipt. The whistleblower should be informed that their concerns have been taken seriously by providing them with a brief overview of the preliminary findings

and an outline of next steps, including any potential timelines and the whistleblower's role moving forward. The organization should also emphasize the company's commitment to confidentiality and protection against retaliation. This communication fosters trust and encourages continued cooperation from the whistleblower.

Lastly, assess whether any employees need to be placed on leave during the investigation. This helps preserve the integrity of the investigation by preventing interference and ensuring an unbiased process. It also protects the whistleblower and other employees from potential retaliation or a hostile work environment, while also minimizing disruption to business operations.



Investigation

Defining the investigation process is one of the more time-consuming portions of designing a whistleblower program. The process should document the timeline of events, parties involved, level of substantiation (fully substantiated, partially substantiated, unsubstantiated), questioned costs (as applicable), and document the findings for any corrective/disciplinary action. A clearly defined process will help standardize the procedures and achieve maximum value from your investigations, so it is important to take the time to thoroughly document the process. For purposes of this white paper, we have broken down the investigation process into the following sections:

- a. Selecting the Investigation Team
- b. Interview Order
- c. Interview Questions
- d. Auditing and Testing

While reporting is also a part of the investigation process, it includes elements outside the investigation, such as communication to the Board and other stakeholders or assistance with next steps. Below is additional detail on the reporting process with key best practices that should be followed during an investigation.

- a. **Selecting the Investigation Team:** The effectiveness of an inquiry largely depends on the expertise and resources available, making it critical to assess the nature of the allegation upfront to determine the appropriate team. For



complex or highly specialized issues, organizations should identify both internal and external subject matter experts with the necessary technical knowledge and investigative skills. Depending on the case, this may include legal advisors, forensic experts (e.g., Certified Fraud Examiners - CFEs), internal audit professionals (e.g., Certified Internal Auditors - CIAs), IT security specialists (e.g., Certified Information Systems Auditors - CISAs), financial analysts, or industry-specific professionals.

When internal resources are insufficient or if there is a need for impartiality, you may opt to pull in outside resources. This process involves identifying reputable external experts or firms with the appropriate credentials and experience to handle the specific allegations. Establishing clear protocols for engaging and integrating these outside resources into the investigation team ensures that all parties work cohesively, and that the investigation remains focused, timely, and credible.



- b. **Interview Order:** Interviews provide firsthand insights and clarify the issues raised in the report. The individuals interviewed and order of interviews should be set and typically follow the below structure. This structured approach helps to build a comprehensive understanding of the situation and ensures that the investigation remains focused and efficient.



Senior Business Leader

Interviewing the senior most business leader will provide an understanding of the organization's stance on ethical issues and whistleblower protections. They can also speak to the character of the individuals involved and serve as an unbiased third party in their assessment of events. This interview should focus on the leader's awareness of the reported issue, their expectations for the investigation, and the company's policies related to the alleged misconduct. It is also important to gauge their commitment to ensuring a fair and unbiased investigation. Discussing the potential impact of the allegations on the organization's reputation, operations, and culture is important, as is exploring any prior incidents of a similar nature that may inform the current investigation.

Whistleblower

The complainant is a central figure in the whistleblower investigation, as their testimony forms the basis of the inquiry. The interview should examine into the specifics of the alleged misconduct, including what they observed, when it occurred, and who was involved. The interviewer should assess the complainant's motivations for coming forward, making sure the complainant understands the investigation process and their rights, including confidentiality and protection from retaliation. Key objectives also include gathering any supporting evidence or documentation the complainant may have and communicating the expectations for the investigation.



Whistleblower's Witness

The complainant's witness can provide corroborative evidence or additional context to support the allegations. This interview should focus on their relationship with the complainant, what they know about the alleged misconduct, and whether they can confirm or clarify any details provided by the complainant. It is also important to explore how they became aware of the issue (i.e., did they witness first-hand, were they told by the complainant, did they overhear office gossip) and their observations regarding the behavior of the accused or other involved parties. Ensuring the witness understands their role in the investigation and that they are protected from any form of retaliation is also crucial.

Accused

The accused individual is a pivotal interviewee, as their perspective and response to the allegations are essential to a fair investigation. This interview should allow the accused to present their side of the story, providing any evidence or explanations for the events in question. Key topics include their relationship with the complainant, their understanding of the allegations, and any relevant context or mitigating factors. Maintain an impartial and non-accusatory tone during this interview to ensure that the accused feels they have an opportunity to fully defend themselves.

Accused's Witness

The accused's witness can offer additional viewpoints that may support the defense or provide further context to the situation. This interview should explore the witness's connection to the accused and their knowledge of the events leading to the allegations. Questions should focus on whether they observed the behavior in question, their assessment of the working environment, and any other relevant information that could either corroborate or refute the claims made by the complainant. As with all witnesses, it is essential to emphasize the importance of honesty and the protection against retaliation.





- c. **Interview Questions:** When conducting interviews, use a structured and strategic approach to ensure the integrity and effectiveness of the process. A funnel approach to questioning — beginning with broad, open-ended questions and gradually narrowing down to more specific inquiries — allows interviewers to establish rapport and gather comprehensive information without leading the interviewee. This technique helps interviewees feel more comfortable and encourages them to share more details. Avoid loaded, trick, or leading questions that might suggest a particular answer or bias the interviewee’s responses. Such questions can compromise the objectivity of the information gathered and undermine the credibility of the investigation.

To ensure that interviews remain focused and unbiased, develop an interview script with questions tailored to the specific context and background information of the case. This preparation enables the interviewer to systematically address key areas of concern while maintaining consistency and fairness throughout the interview process. By combining a thoughtful question sequence, avoiding biased questioning techniques, and preparing thoroughly, investigators can enhance the reliability of their findings and contribute to a more effective anti-fraud program.

Below is a potential interview outline with example questions for context. In the appendices to this report is an [Investigation Interview Script](#).



	✓ Purpose	? Example Questions
Introductory	Introduces relevant parties, explaining the purpose of the interview and setting the ground rules. This phase is crucial to build trust and make the interviewee comfortable.	Interviewer will typically introduce themselves and provide context for discussion. <ul style="list-style-type: none"> "Can you please confirm your name and role?"
Background	Get the interviewee talking about their background, role, and responsibilities. This helps to establish a baseline for their knowledge and experience. Questions are generally open-ended.	<ul style="list-style-type: none"> "Can you tell me about your role and responsibilities in the company?" "Can you tell me about the size of your team and who you work with in your day-to-day?"
Contextual	Ask questions to understand the context surrounding the whistleblower's report or the allegations being investigated. This is typically a mix of open and closed ended questions.	<ul style="list-style-type: none"> "Have you observed any unusual activities or behaviors recently?" "Are there any areas of concern you have regarding internal controls, operations or otherwise?" "What prompted you to raise this concern?"
Incident Specific	Dive into the details of the specific incidents that have been reported. Ask fact-based, open-ended questions to allow the interviewee to describe what they know or have experienced.	<ul style="list-style-type: none"> "Can you describe in detail what you observed or experienced?" "Were there other parties present to this incident?"
Clarifying and Probing	After the initial recounting of events, ask follow-up questions to clarify details, verify timelines, and gather more in-depth information. Probing questions help to fill gaps and uncover more specifics.	<ul style="list-style-type: none"> "Can you clarify what you meant when you said...?" "Can you recall the exact date and time of this incident?"
Exploratory	Understand the potential motivations behind the reported behavior and explore any broader implications for the organization.	<ul style="list-style-type: none"> "What do you think could have caused this or why do you think this happened?" "Do you believe there are any other incidents related to this issue?"
Verification and Cross-Reference	Verify the credibility of the information provided and cross-check it with other sources or evidence.	<ul style="list-style-type: none"> "Can you provide any documents or evidence to support your claims?" "Are there any other witnesses who can corroborate what you've told me?"
Concluding	Summarize the interview, ensure nothing important has been missed, and provide the interviewee with an opportunity to add any final thoughts.	<ul style="list-style-type: none"> "Is there anything else you think I should know about this situation?" "Do you have any concerns or suggestions for improving our processes?"





- d. **Auditing and Testing:** Auditing and testing helps validate the concerns raised and provides concrete evidence to support findings. The interview process often informs the testing procedures, revealing areas that require closer examination or specific transactions that need to be scrutinized. To ensure the accuracy and reliability of the results, define a clear sampling methodology and select samples that are representative and relevant to the issue at hand.

Once testing is complete, all findings must be thoroughly documented and supported with adequate evidence. This documentation serves as the backbone of the investigation, providing transparency and accountability while also protecting the organization from potential disputes or challenges. Clear and detailed records ensure that the conclusions drawn from the investigation are defensible and can be relied upon to inform any necessary corrective actions.

4 Reporting

The primary goal of any investigation report is to present the facts objectively, allowing decision-makers to understand the situation and take appropriate action without prejudice. Reports that rely on clear, well-documented evidence rather than assumptions or opinions help maintain credibility and avoid potential legal challenges. Unbiased reporting also ensures fairness to all parties involved, including the whistleblower and those implicated, by preventing undue influence on the investigation's findings. Ultimately, precise and impartial documentation fosters trust in the whistleblower program, encourages future reporting of unethical behavior, and upholds the organization's commitment to transparency and accountability.



Reports can be issued in varying length, depending on the nature, scope, objectives, and findings, however, they should contain the following general sections/information:

Background	Provides context for the investigation by outlining the origin of the complaint, the individuals or departments involved, and the initial information received, helping readers understand the circumstances that led to the investigation.
Executive Summary	Offers a concise overview of the investigation, including key findings, conclusions, and recommendations, allowing stakeholders to quickly grasp the report's most critical aspects without reading the entire document.
Scope	Defines the boundaries of the investigation, including what issues were examined, what was excluded, and any limitations encountered, ensuring that the report's focus and objectives are clear.
Approach / Procedures Performed	Describes the methods, techniques, and steps taken to gather evidence and conduct the investigation, providing transparency and demonstrating the rigor and thoroughness of the process.
Findings	Details the facts uncovered during the investigation, including evidence of misconduct or unethical behavior, organized in a way that supports the conclusions drawn and maintains objectivity.
Impact to Books (as applicable)	Assesses the potential financial impact or discrepancies identified in the company's financial records because of the misconduct, which is necessary to understand the broader implications of the findings.
Recommendations and Corrective Action	Suggests specific steps that the organization should take to address the issues uncovered, prevent future occurrences, and improve internal controls or policies, guiding management toward effective remediation.



Level of Substantiation

In whistleblower investigations, levels of substantiation refer to the degree of evidence found to support the claims made. A “substantiated” finding means the allegations are proven true, based on clear and credible evidence. A “partially substantiated” result indicates that some, but not all, aspects of the allegations are supported by evidence, suggesting partial truth or validity. On the other hand, an “unsubstantiated” finding means that the investigation did not uncover sufficient evidence to support the claims, and the allegations cannot be confirmed. These levels guide the decision-making process and outcomes of investigations, helping determine the appropriate actions to take.

The percentage of whistleblower complaints that end up unsubstantiated can vary significantly depending on the industry, the organization, and the nature of the allegations. However, some general estimates from various studies and reports suggest that a substantial portion of complaints are ultimately found to be unsubstantiated or not corroborated. The results can differ across industries. For example, in sectors where whistleblowers are more likely to report financial fraud or misconduct, a higher percentage may be unsubstantiated due to a lack of direct evidence. In contrast, in industries focused on workplace safety, more claims may be substantiated. Ultimately, while there’s no universal statistic, a reasonable estimate would be that anywhere between 30-60% of complaints could be unsubstantiated, with varying degrees depending on the context and the thoroughness of the investigation process.



5 Close Out

Review Investigation Report and Inform Relevant Stakeholders of Outcomes: This step ensures that key stakeholders are fully aware of the findings, conclusions, and potential implications of the investigation, allowing them to make informed decisions and take appropriate actions to address the issues identified. Key stakeholders may include:

- **Senior Management:** Senior management needs to be informed of investigation results to make informed decisions on corrective actions, policy adjustments, and resource allocation to address any identified risks or issues.
- **Board of Directors:** The Board of Directors requires investigation results to fulfill their governance responsibilities, ensuring that proper oversight and strategic guidance are provided, particularly in high-risk or compliance-related matters.
- **Enterprise Risk Management:** Enterprise Risk Management may need to be informed to evaluate the impact of the findings on the organization's risk profile and to incorporate the results into broader risk mitigation strategies.
- **Internal Audit:** Internal Audit should be informed to assess the effectiveness of internal controls and determine if the results indicate any systemic issues that may require further auditing or oversight.

Respond to Whistleblower and Notify the Accused of Next Steps: Communicating the outcomes to the whistleblower helps maintain transparency and trust

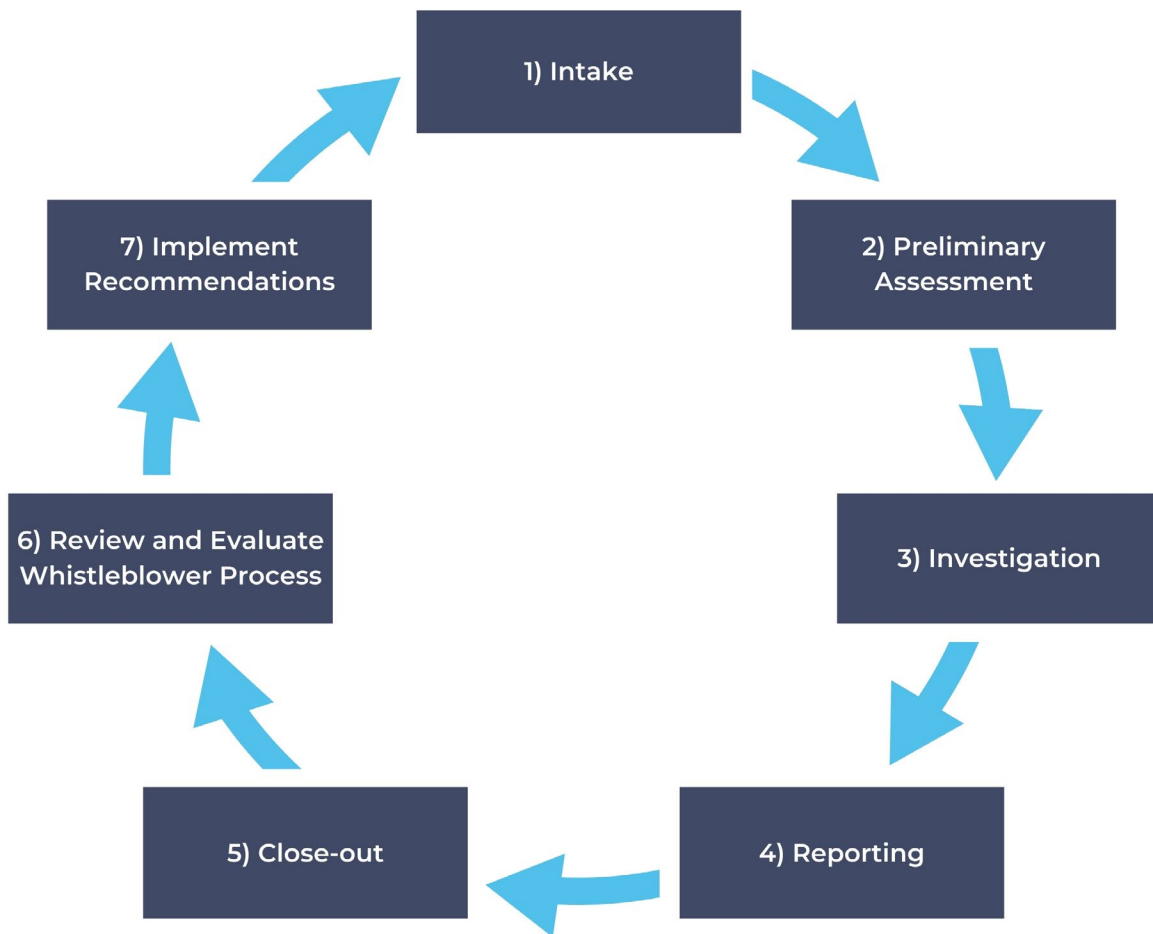
in the whistleblower process. Notifying the accused of the findings and next steps ensures fairness and clarifies any further actions or proceedings.

Take Disciplinary/Remedial Action as Deemed Necessary: Implementing appropriate disciplinary or remedial actions based on the investigation's findings may be necessary for addressing misconduct, deterring future unethical behavior, and reinforcing the organization's commitment to maintaining ethical standards and a safe, compliant work environment.



Continuous Monitoring and Improvement

Detection and prevention of fraud requires ongoing effort and vigilance. Continuously evaluating and refining the whistleblower system ensures that the program remains responsive to emerging risks and aligns with best practices, thereby enhancing overall operational effectiveness. Adequately designed programs that include regular assessments and feedback loops help identify areas for improvement, streamline processes, and reinforce a culture of ethical behavior. Furthermore, transparent communication of investigation results to relevant stakeholders not only fosters accountability but also provides valuable insights that can drive policy changes and strengthen internal controls, contributing to a more resilient and proactive organizational environment.



Steps 1-5 are described in detail in the [Whistleblower Process Section](#)

Step 6: Review and Evaluate Whistleblower Process

Periodic evaluations of the whistleblower program help to ensure continuous improvement of the program over time. Evaluations can be performed after an individual investigation to provide a micro (process-level) view, as well as on a consistent, periodic basis (i.e., annually) to provide a macro view (program-level). The evaluation should consider key performance indicators at the program-level and process-level. Many process-specific KPIs can also be evaluated at the program-level. Examples include:

Program-Level Key Performance Indicators

- **Number of Reports Submitted:** Tracks the volume of whistleblower reports received over a period, indicating the awareness and utilization of the whistleblower program.
- **Report Categories and Types:** Analyzes the types of issues being reported (e.g., fraud, harassment, safety violations) to identify prevalent risks and areas that need targeted intervention.
- **Percentage of Anonymous Reports:** Evaluates the proportion of reports submitted anonymously, which can indicate the level of trust employees have in the confidentiality of the whistleblower system.

- **Substantiation Rate of Reports:** Assesses the percentage of reports that are found to be credible or substantiated after investigation, providing insight into the quality and seriousness of the allegations being reported.
- **Employee Awareness and Training Rates:** Measures the percentage of employees who have received training on the whistleblower policy and procedures, indicating the program's reach and effectiveness in promoting awareness.

Process-Level Key Performance Indicators

- **Time to Resolution:** Measures the average time taken from the receipt of a report to the closure of the investigation, reflecting the efficiency of the investigation process and responsiveness of the program.
- **Feedback and Satisfaction Scores:** Gathers feedback from employees who have used the whistleblower system regarding their experience and satisfaction, highlighting areas for improvement.
- **Communication and Outcome Transparency:** Evaluates how well the outcomes of investigations are communicated back to stakeholders, including steps taken and improvements made, which can help build trust and demonstrate the program's impact.
- **Compliance Considerations:** Assesses whether the organization complied with relevant requirements throughout the whistleblower process (i.e., the EU Whistleblower Directive mandates acknowledging receipt of report to whistleblower within 7 days of receipt).



- **Number of Interviews Conducted:** Assesses the number of interviews conducted per investigation, indicating the depth and comprehensiveness of the fact-finding process.
- **Quality of Evidence Collected:** Evaluates the quality and reliability of evidence gathered during the investigation, which is crucial for substantiating findings and making informed decisions.
- **Investigation Outcome Rate:** Tracks the outcomes of investigations (e.g., substantiated, unsubstantiated, inconclusive), which helps in understanding the effectiveness of the investigative process and/or quality of the allegations received.
- **Compliance with Investigation Procedures:** Assesses adherence to established protocols and guidelines during the investigation, ensuring consistency and fairness.
- **Rate of Corrective Actions Implemented:** Monitors the percentage of investigations that lead to corrective actions, reflecting the impact and effectiveness of the investigation process.
- **Investigation Cost:** Analyzes the total cost incurred for each specific investigation, helping assess resource allocation and financial efficiency.

Step 7: Implement Recommendations to Whistleblower Process

Thoroughly analyze the KPI data to identify gaps, inefficiencies, and areas needing improvement, such as response times, training effectiveness, or the quality of investigation outcomes. Based on this analysis,

develop specific and actionable recommendations, prioritizing those that address high-risk areas or have the most significant impact on program effectiveness. Involve key stakeholders in the planning phase to ensure buy-in and to allocate resources appropriately. Once recommendations are approved, they should be implemented through a structured action plan that includes clear timelines, responsible parties, and measurable targets. Regular follow-up and reassessment of KPIs are necessary to monitor the effectiveness of the changes and to make further adjustments as needed, ensuring the whistleblower program remains robust, responsive, and trusted.





Closing Thoughts

Implementing a comprehensive whistleblower program is a strategic decision that aligns risk mitigation and fraud prevention goals. Establishing strong governance and fostering a supportive organizational culture encourages early detection of misconduct, allowing organizations to address potential risks before they escalate. By embedding a whistleblower program into the company's broader risk management strategy and anti-fraud program, organizations can better align with regulatory expectations and proactively manage reputational risks associated with unethical behavior. This alignment ensures that organizations are not only compliant with legal standards but are also resilient in the face of emerging challenges.

A robust whistleblower process, covering intake, assessment, investigation, reporting, and close-out, provides a structured and transparent approach to handling allegations of misconduct. Clear reporting and follow-up mechanisms contribute to

an environment where employees feel empowered to speak up, enhancing the organization's ability to detect and respond to potential threats. Continuous monitoring and improvement based on data-driven insights help organizations refine their approach over time, ensuring the program remains effective and responsive to changing risk landscapes. This proactive stance supports the long-term sustainability of the organization by safeguarding its assets, reputation, and stakeholder trust.

The benefits of a well-designed whistleblower program extend beyond compliance; they provide valuable insights into internal controls, strengthen ethical standards, and promote a culture of accountability. Organizations that commit to ongoing evaluation and enhancement of their whistleblower processes position themselves to not only prevent and detect fraud but also to foster an environment of transparency and integrity. This forward-looking approach can serve as a competitive advantage, building confidence among investors, customers, and employees while reinforcing the organization's commitment to ethical business practices.





CPAs & ADVISORS

GRF Can Help

With more than 40 years of experience serving nonprofits and associations, GRF is here to support your organization. GRF CPAs & Advisors provides a full suite of audit, accounting, tax, and advisory services to clients worldwide.

Our risk & advisory experts can help you address today's emerging risks:

Internal Audit and Investigations



GRF has seen a sizable increase in fraud among our nonprofit and association clients. A fraud risk assessment can help your organization prevent and detect fraudulent activity. This assessment identifies the processes that could be exploited (for example, due to lack of controls or staffing constraints) and focuses on these and other high-risk processes, such as accounts payable and expense reimbursement. This enables your organization to allocate resources to mitigating the most significant risks and develop a monitoring plan for less significant risks. A fraud risk assessment feeds into an internal audit plan to mitigate risks and identify opportunities for process improvements. If you suspect fraud has occurred, GRF's certified fraud examiners can investigate allegations and recommend remedial actions.

Whistleblower Investigation Services



GRF's team of professionals regularly investigates sensitive issues raised by whistleblowers, helping you understand the facts and circumstances, risks, and corrective action needed to properly resolve a whistleblower complaint. We work closely with your legal counsel, human resources professionals, compliance leaders, and other stakeholders to create an appropriate work plan and path forward.

You can reduce costs through our expedited, focused action. We will assess the merit of allegations, develop targeted testing based on scope and duration of investigation, and develop recommendations tailored to your operations. We can also assist in developing policies and processes to build an effective whistleblower program.



CPAs & ADVISORS

Resources and References

Association of Certified Fraud Examiners. (2024). *2024 Report to the Nations*. Retrieved from <https://www.acfe.com/-/media/files/acfe/pdfs/rtn/2024/2024-report-to-the-nations.pdf>

Association of Certified Fraud Examiners. (n.d.). *Building a Best in Class Whistleblower Hotline Report*. Retrieved from <https://www.acfe.com/fraud-resources/whistleblower-hotline-report>

Institute of Internal Auditors. (2024). *2024 Pulse of Internal Audit*. Retrieved from <https://www.theiia.org/en/resources/research-and-reports/pulse/>

NAVEX 2024 Whistleblowing & Incident Management Benchmark Report https://www.navex.com/en-us/northstar/whistleblowing-incident-management-benchmark-report/assets/v4_navex_benchmark_report.pdf

The Institute of Internal Auditors, The American Institute of Certified Public Accountants, and Association of Certified Fraud Examiners, *Managing the Business Risk of Fraud: A Practical Guide*. Retrieved from <https://us.aicpa.org/content/dam/aicpa/forthepublic/auditcommitteeeffectiveness/guidanceandresources/downloadabledocuments/managing-the-business-risk-of-fraud.pdf>

U.S. Securities and Exchange Commission. (2023). *FY23 Annual Report*. Retrieved from <https://www.sec.gov/files/fy23-annual-report.pdf>

Sarbanes-Oxley Act (SOX), Section 301(m)(1)(4)(a-b). Retrieved from https://pcaobus.org/About/History/Documents/PDFs/Sarbanes_Oxley_Act_of_2002.pdf

European Parliament and Council. (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*. Retrieved from <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L1937>

GRF CPAs & Advisors: How to Set Up a World-Class Whistleblower Program Webinar Series

- **Part 1: Setup and Implementation** - <https://www.grfcpa.com/resource/how-to-set-up-a-world-class-whistleblower-program/>
- **Part 2: Reporting** - <https://www.grfcpa.com/resource/how-to-set-up-a-world-class-whistleblower-program/>
- **Part 3: Wrap Up** - <https://www.grfcpa.com/resource/part-3-how-to-set-up-a-world-class-whistleblower-program/>

Superscript references:

3-5¹ is the minimum number of people needed to achieve quorum in a voting situation and limits the number of individuals with access to the sensitive details of whistleblower allegations. However, larger, more complex organizations may require multiple councils across different regions and/or additional subject matter experts to thoroughly evaluate each allegation and ensure the program participants are not overburdened. The committee can also designate a backup to serve in the event an allegation is received regarding one of the committee members.



Glossary of Key Terms

COSO (Committee of Sponsoring Organizations)	A joint initiative providing a framework for organizations to manage risk, control processes, and enhance governance.
ACFE (Association of Certified Fraud Examiners)	A global professional body dedicated to training and certification in fraud detection, prevention, and investigation.
IIA (Institute of Internal Auditors)	A global organization offering standards, guidance, and certification for the internal audit profession.
ISACA (Information Systems Audit and Control Association)	A global association focused on IT governance, cybersecurity, risk management, and audit for information systems.
ESG (Environmental, Social, and Governance)	A framework used to assess a company’s practices related to sustainability, ethical impact, and governance transparency.
SME (Subject Matter Expert)	An individual with in-depth knowledge or expertise in a specific field or topic.
Access Management	<p>The process of controlling and managing user access to systems, networks, and data within an organization.</p> <ul style="list-style-type: none"> • Role-based access: A security approach that assigns system access based on a user’s role within the organization. • Encryption: The process of converting data into a coded format to prevent unauthorized access. • Multi-Factor Authentication: A security measure that requires multiple forms of verification before granting access to a system or application.
Independence and Objectivity	<p>The ability to perform tasks or evaluations without bias or undue influence, ensuring impartiality in decision-making.</p> <ul style="list-style-type: none"> • Independence: The freedom from external influence or pressure, allowing an individual or organization to perform duties or make decisions without being affected by conflicts of interest. • Objectivity: The ability to remain impartial and unbiased when making decisions or assessments, relying on facts and evidence rather than personal opinions or external pressures.



Glossary of Key Terms

<p>Confidentiality and Anonymity</p>	<p>The protection of sensitive information and ensuring that whistleblowers can report concerns without revealing their identity.</p> <ul style="list-style-type: none"> • Confidentiality: The responsibility to protect sensitive information from unauthorized disclosure, ensuring that details are only accessible to those who need to know. • Anonymity: The protection of an individual's identity, ensuring that their personal information is not disclosed or associated with a report or action, especially in the context of whistleblowing.
<p>Fraud</p>	<p>Deliberate deception intended to secure an unfair or unlawful gain, often resulting in financial or reputational damage</p>
<p>Employee Misconduct</p>	<p>Actions by employees that violate company policies, ethical standards, or legal requirements.</p>
<p>Tone-at-the-top</p>	<p>The ethical climate and culture set by an organization's leadership, which influences employee behavior and organizational integrity.</p>
<p>Global Internal Audit Standards</p>	<p>A set of internationally recognized principles and guidelines for the internal audit profession, established by the IIA.</p>
<p>Key Performance Indicator (KPI)</p>	<p>A measurable value that demonstrates how effectively an organization is achieving its strategic and operational objectives.</p>
<p>Fully Substantiated</p>	<p>A whistleblower claim that has been thoroughly investigated and supported by conclusive evidence.</p>
<p>Partially Substantiated</p>	<p>A claim that has been investigated and partially supported by evidence but lacks complete verification.</p>
<p>Unsubstantiated</p>	<p>A claim that has been investigated but found to have insufficient or no evidence to support the allegation.</p>
<p>Chief Audit Executive (CAE)</p>	<p>The senior executive responsible for overseeing an organization's internal audit function and ensuring the effectiveness of its internal controls.</p>
<p>Chief Risk Officer (CRO)</p>	<p>The executive responsible for identifying, assessing, and mitigating risks across an organization to ensure its long-term success and resilience.</p>



Appendices

Individuals Interviewed

We extend our heartfelt gratitude to all those who contributed their time, expertise, and insights to this paper. Their valuable input has been instrumental in shaping the content and enhancing its quality.

- **Matt Kelly**
Founder of Radical Compliance
- **Elizabeth J. Folsom, MBA, CPA/CFE, CIA, CFE, CCSA, CRMA**
Chief Audit Executive at Population Services International
- **Vasanthi Ramkumar, CPA, CGMA, CISA, FCA**
Head of Internal Audit at Helen Keller International
- **Rebecca Mason**
Senior Ethics and Compliance Investigations Manager

Templates

- [COSO Fraud Risk Management Template](#)
- [Whistleblower Allegation Listing Template](#)
- [Whistleblower Investigation Detail Template](#)
- [Whistleblower Investigation Interview Script](#)

