



A NAVEX **One**® Definitive Guide



# Definitive Guide to Incident Management

- Going Beyond the Whistleblower Hotline



# Contents

## Introduction

Why is an Incident Management Program Important?	3
A Strong Incident Management Program Addresses Concerns from All Sources	4
The Benefits of a Comprehensive Incident Management Program	5

## Plan

Define Program Goals and Create a Strategy	7
Critical Components to Include in Planning for the Incident Management Program	7
Internally Staffed Vs. Third-Party Hotlines	10
Who Should “Own” the Incident Management Program?	10
Who Should Enter a Report Into the Incident Management System?	11
How Reports are Disseminated	11
Quality Metrics	12
Escalation Criteria – Two Separate Approaches Needed	12
Special Considerations for Global Operations	13
Data Security and Retention	14

## Implement

Promote Use of the Incident Management Program	15
Use Multiple Delivery Methods for Awareness	15
Launching the Program	16
After the Call – Responding to Reports	17
Investigating Allegations	18
Tracking the Progress and Outcomes of Reports	18
Recognition and Information Publication	19
When The Incident Management Program is ‘Stuck in Neutral’	19
Root Cause Diagnosis: Program Awareness and Communications Missing the Mark	20
Solution: Delivering the Right Message to the Right Audience at the Right Time	20
Awareness and Communications Planning and Execution Essential for Program Success	20

## Measure

Monitor and Improve Program Effectiveness	21
Benefits of Monitoring the Incident Management Program	21
Measuring Program Effectiveness With Benchmarking	22

## Conclusion

23



# Overview

## **This Definitive Guide to Implementing an Effective Incident Management**

**Program** is a comprehensive resource full of tips, advice and examples to help companies implement and manage effective ethics and compliance intake and reporting programs.

Organizations with a strong intake and incident management program have better visibility into employee concerns enterprise-wide, become proactive in mitigating risks and protect their reputation and bottom line.

This guide is divided into three main sections: **PLAN, IMPLEMENT, and MEASURE**. Each section provides important information and tools needed for a strong foundation for incident management.

# ■ Introduction

## Why is an Incident Management Program Important?

Research continues to show that organizations with strong ethical cultures have lower rates of witnessed misconduct. By implementing an incident management program, organizations are asking and encouraging employees and third parties to inform them of potential unethical behavior. They are demonstrating their commitment to operate ethically. Moreover, a higher level of reporting contributes to better business outcomes. While this may seem counterintuitive at first glance, higher levels of reports indicate trust in the system, and provide valuable insights into the culture of the business. The information included in incident reports signals areas of risk that business leaders should address as opportunities to achieve a consistently ethical culture.

An effective incident management program does more than reduce organizational risk. Requesting and addressing employee concerns and potential misconduct creates a culture of trust and respect. When employees can raise concerns confidentially or anonymously, and see those issues addressed, they build confidence that their requests will be handled and resolved using a consistent and fair process.



### **An organization's hotline reporting system serves many purposes, such as providing:**

- A confidential place for employees to clarify policy and discuss or report concerns
- A communications channel beyond the rumor mill
- A way to direct employee questions to the appropriate resource
- An opportunity to provide guidance before a poor decision is made
- An early warning of issues or problem areas brewing in the organization
- An unfiltered source of ground-level risk data powered by direct employee input
- A last internal stop for whistleblowers before they take an issue outside the organization to a regulator or attorney

## A Strong Incident Management Program Addresses Concerns from All Sources

Organizations are at a disadvantage when it comes to learning about misconduct within their ranks. There are many reasons employees are reluctant to share their questions or concerns: fear of retaliation and cynicism that a report will not be taken seriously are among the top reasons employees don't report.

Complicating matters, when employees do report – which includes anything from questions about a policy or procedure to allegations of misconduct – those reports might never make it on the radar of compliance professionals.

Why? Because while hotline/helpline and web intake forms are automatically captured in a centralized incident management system, other reporting methods – email, mail, fax, or reports made in-person to human resources or a manager, for example – are typically not. Among these, the biggest missed opportunity for report capture is how organizations document and track in-person reports to managers.

Consider this: In 2021, organizations that only tracked web and hotline reports averaged .9 reports per 100 employees. Conversely, organizations that tracked “all other” reporting channels (primarily open-door reporting) saw a median reporting rate of 1.7 reports per 100 employees.

When employees have options to report their concerns or make inquiries, they are more likely to do so. This in turn gives the organization valuable insights into the company culture and demonstrates a commitment to ethics and compliance.



**A strong incident management program can track reports from all channels to provide an accurate, holistic view of E&C cases and the cultural health of the organization.**

Though a hotline/helpline is a central piece of an effective incident management system, it is not sufficient by itself. Organizations should offer at least three reporting options:

- 1 Hotline.** Whether a hotline reporting program is mandated for the organization or not, it is still a standard and expected practice component of any ethics and compliance program. Think of it as a “canary in the coal mine.” It is often through hotlines that employers find out whether training is effective, where they have gaps in their policies and whether there are critical cultural issues that need to be addressed so misconduct does not take root.
- 2 Web-based reporting.** Some employees do not feel comfortable speaking with a live operator about their issue or do not have a private location available to make a call. With web-based reporting, employees can type information into an online form and take time to think about and review what they have written before submitting. A web-based portal should be accessible from any device, and be secure, confidential, and accessible 24 hours a day.
- 3 Open-door intake.** This is a web-based tool that allows every manager and some departments, such as HR and legal, to input reported issues and actions taken into an organization’s ethics and compliance (E&C) incident management system. Since research shows that most reports are captured during in-person meetings with managers, this is one of the most critical components of a reporting system.

A comprehensive incident management program provides:

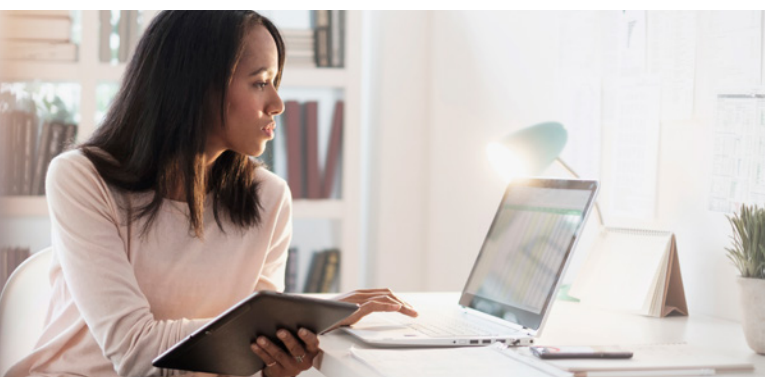
- A variety of mechanisms for employees to ask questions or raise issues. These include reporting to a manager or higher up in the organization, as well as to human resources, legal and the ethics and compliance office via a 24/7/365 phone or web intake process.
- Tracking and case management processes to make sure reported incidents are collected in a centralized location, resolved in a timely manner and accurately reported – no matter where they originate.
- Access to a centralized data source to identify trends and gaps in the ethics and compliance program, determine where training is needed, locate “hot spots” within the organization and update any unclear or outdated policies.

## The Benefits of a Comprehensive Incident Management Program

A comprehensive incident management system allows an organization to capture, investigate and manage ethics and compliance reports from across the organization, regardless of reporting channel, in a centralized database.

With a strong incident management program organizations are well positioned to:

**Create a strong ethics culture.** Set the expectation that every employee report is a critical piece of business intelligence. Resolving incident reports consistently and updating policies as a result improves employee trust in the organization. Employees know their issues will be addressed, creating a stronger culture and more engaged employees.



**Get better visibility into risk.** The 2022 NAVEX Hotline Benchmark Report found organizations that document reports from all channels receive nearly double the median amount of reports per employee than those that just track from web-based and hotline reports. More reports being captured means more risk visibility – and more opportunity to spot trends and act on emerging problem areas.

**Go deeper.** Analyze incident reporting data by manager, location, business unit or department to further pinpoint areas of concern. Only looking at top line, organization-wide data is a missed opportunity. The real value in analytics is looking at variances across the organization and highlighting those locations, operating units or geographies that are varying significantly higher or lower than the norm of the organization. A deep dive offers actionable data for leadership to review and address.

**Offer tailored training.** Use data about where concerns and misconduct are occurring to offer specific training to individuals or groups as needed.

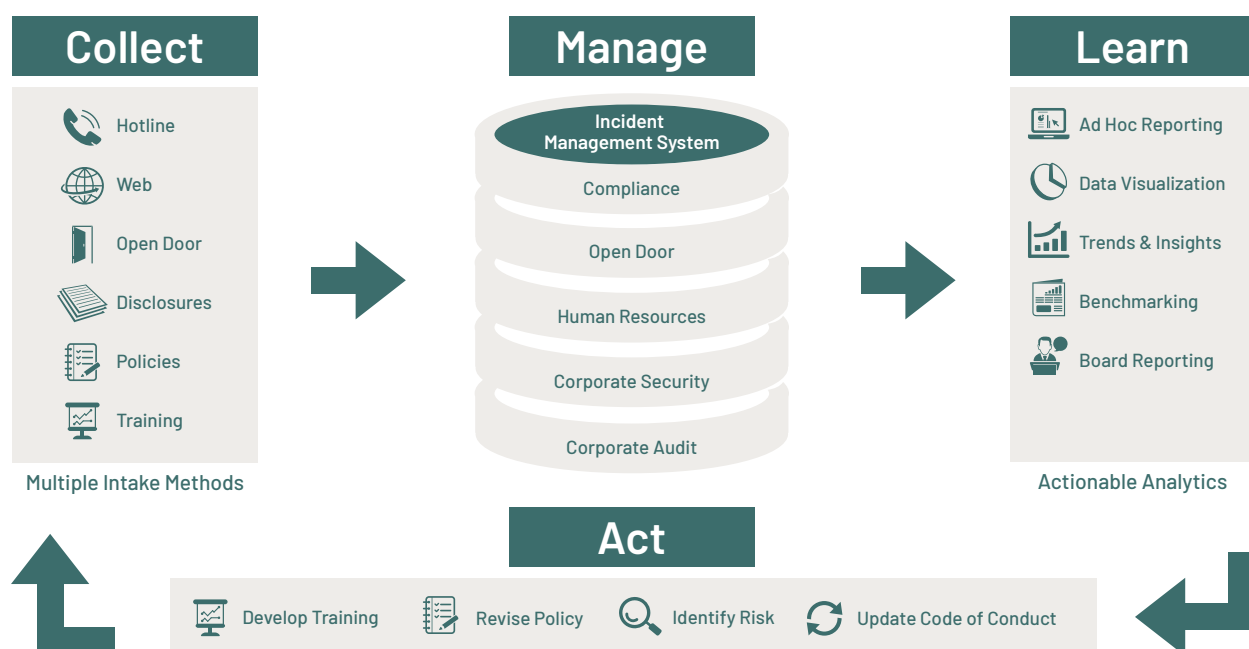
**Update policies and code of conduct.** A strong centralized program allows the compliance officer to see when policies or the code of conduct have become outdated or are unclear.

**Bring consistency and uniformity to a core compliance process.** From a reporter's perspective, working within a comprehensive, standardized incident management system provides a more structured and predictable experience.

**Be audit ready.** A comprehensive program – supported by centralized software – ensures the organization has a defensible audit trail should there be any question about how cases were consistently investigated and resolved.

**Track program effectiveness.** Trends in reporting vary year over year, keep up with industry trends and benchmark against your peers.

## Incident Management: The Core of an E&C Program







# ■ Plan

## Define Program Goals and Create a Strategy

The first step in developing a strong incident management program is to define the goals and objectives of the program. These objectives vary among organizations and will impact the implementation and communication strategies of the program.

Following are 10 questions to consider:

- 1 What results does the organization want to achieve with the program?
- 2 Who is the sponsor and owner of the program?
- 3 Who are the key stakeholders to be involved in the planning and implementation process?
- 4 What is the role of leadership and the board of directors in establishing, overseeing and monitoring the program?
- 5 Will the program encourage employee questions and input or only request allegations of wrongdoing? Best practice is to encourage all types of contacts.
- 6 How does your organization promote awareness and availability of the reporting channels?
- 7 How will the results and outcomes of reports received be measured and reported?
- 8 How will ongoing program quality and effectiveness be monitored?
- 9 Will the organization publish sanitized statistics regarding the numbers and types of issues raised through the program? Best practice is to do so.
- 10 How will the organization address and respond to concerns of retaliation?

## Critical Components to Include in Planning for the Incident Management Program

Once the goals and objectives are defined, the planning process can move into strategy development. Setting up a toll-free number and a website are only a small part of the process. What is done with the information once it is received drives the credibility of the program within all levels of the organization.

When creating and planning for the incident management program, consider the following critical components to help ensure success.

**Secure top-down support.** Visible support from top executives is critical in any program seeking to influence or modify employee behavior. If a program is seen as unimportant, a nuisance or a threat to top management, employees will not trust it or use it. Ensure there is alignment among the board of directors and senior management on the use and value of the program.

**Define stakeholder involvement.** Stakeholders in the program should include legal, finance/audit, human resources, risk management, loss prevention (if applicable), operations, information technology (IT) and communications. Stakeholders should discuss the implementation plan, timeframe, resources and



any enhancements that would make the program more valuable. In addition, the board of directors needs to be aware of the program and may wish to provide some specific direction regarding operations.

Ensure each stakeholder has a clearly defined role in the program. If there is ambiguity about responsibilities, the process could break down or result in unproductive confusion over role requirements. Investigation plans and protocols as well as a triage process will need to be in place for all types of reports that may be received.

Develop and document a protocol for report investigation that defines who will lead the investigation, who will review the outcomes and who will make and implement disciplinary recommendations and decisions. Develop a formal escalation policy defining what the leadership and board of directors needs to know and when.

**Know the regulatory requirements that could affect the program.** Whether it is data privacy and protection, dedicated reporting channels and investigative resources as required by the EU Whistleblower Directive or other national whistleblowing law, or required protections against retaliation, the regulations that impact the operation of an incident management program are far-reaching and complex. Ensure your planning addresses all regulatory requirements early in the process to avoid costly and time-consuming delays in the implementation process.

**Carefully consider program branding.** The language an organization uses (formally and informally) to describe its program will affect employees' comfort and confidence in the program. Align with leadership on how and when they expect the process to be used. Best practice organizations welcome questions and concerns via their reporting system.



When possible, avoid using the term “whistleblower” when describing the process or employees with concerns. Instead, consider messaging that is more open and welcoming, such as “integrity line” or “ethics helpline.” Also consider using the same branding as used in the code of conduct and awareness materials. The same “look and feel” will help identify the various program resources available to employees.

**Offer a variety of methods for reporting that do not require “chain of command” reporting.** While some people feel comfortable coming forward through an open-door policy, others may not. Some employees are hesitant to reveal their identities – or to report at all – because they fear retaliation or because they assume no one will act on the report. Offer a range of reporting options including hotline, web-based, email, postal mail, and open-door intake to capture incidents. Offer the hotline reporting mechanism as one avenue that employees have to report issues or concerns, rather than as a “last resort.”

**Consider offering one reporting “ecosystem”.** Having multiple reporting numbers or sites for different issues is not only a burden from an administrative perspective, it can confuse employees, suppliers, consumers and other stakeholders. An organization can quickly alienate potential reporters if complaints regarding discrimination and sexual harassment – both high liability issues – are turned away because the website or hotline is “for corruption and bribery complaints only.” It is better to learn about high liability issues as early as possible so that the organization can investigate and remediate to avoid legal action. Therefore, having a single, unified system in place gives organizations a better opportunity to limit their liability.

**Capture the most complete and accurate information.** Especially in the case of anonymous reporters, there may never be an opportunity to ask clarifying questions. Top tier third-party hotline providers are well equipped to ensure all important details are captured with trained, vetted hotline interviewers and web-based reporting tools while protecting the identity of confidential callers. When follow-up is necessary, third-party providers also have a system for offering unique identifier codes so anonymous reporters can get back in touch. It is critical to train employees on their responsibility to follow up on anonymous reports.

**Offer a third-party “staffed” reporting approach to ensure 24/7/365 coverage.** Some companies rely on a voicemail box or an anonymous e-mail that employees can use to send in “tips.” This is a mistake and missed opportunity because it can lead to missing information and gives employees the impression that the program is low priority.

Interactive communication, such as a face-to-face conversation or a hotline interview, generates much more actionable information than one-way communication. Having a staffed hotline also gives employees confidence that the organization is taking the program seriously and that any concerns they bring forward will be addressed. Further, in support of international operations, translations services should be provided.



**Take anonymous reports seriously.** Occasionally, senior leaders and board members can be biased against the acceptance of anonymous reports. However, research has shown that names are withheld typically out of fear of retaliation or a desire to not be involved – not because the issue reported is deliberately false or frivolous.

In fact, the 2022 NAVEX Hotline Benchmark report found that the substantiation rate (those allegations which were determined to have at least some merit) for anonymous reports was 39 percent. This is on par with the past several years’ substantiation rates which are typically close to 40 percent. This demonstrates that these reports are valuable and credible.

**Before taking any reports, develop an investigations protocol and ensure sufficient resources are available to train all investigators on the right way to conduct an investigation.** Nothing is worse for an incident management program than a bungled investigation. Serious errors can be costly and can destroy careers, lives and reputations. They could also violate somebody’s rights. Thoughtful investigation protocols provide consistency in approach, and trained investigators are much better able to provide actionable and defensible information to leadership. Build time into the process to ensure all who will touch and investigate a report are proficient and that all stakeholders are protected.

Further, investigations that drag on for months with no ongoing communication with the reporter does significant harm to the credibility of the organization and the program. Plan with all investigating organizations to have sufficient resources available to handle the expected volume of reports as well as the need for regular updates to the appropriate people.

**Adopt a mentality of protecting the accuser and the accused equally.** Confidentiality of investigation information is critical to protecting employees and the organization. In planning and development of

protocols, carefully consider who really needs to know the names of the accuser and the accused before, during and after the investigation. Be thoughtful about forwarding an entire case report if the recipient does not need to know specific names.

### **Be prepared to train on, manage and monitor**

**for retaliation.** Every organization should have a written formal policy against retaliation for reporting misconduct and for participating in investigations into misconduct. If retaliation happens, there should be a clear process for investigating and addressing it. Ensure that employees are aware – through venues such as regular compliance training, online burst learning and staff meeting discussions – that the organization will not tolerate retaliation. Talk about the steps to take if someone does suspect retaliation. Finally, consider developing a practice of proactively monitoring for retaliation and publicize the fact that it is happening to serve as a deterrent.

**Think ahead.** How will ongoing support and communication requirements be managed? Is there a plan for evaluating and periodically assessing and redirecting the program? Continuous monitoring of the program helps plan for improvements to ensure its success.

## **Internally Staffed Vs. Third-Party Hotlines**

The majority of organizations today use a third-party staffed hotline. That's because a professional third-party hotline provider comes with expertise, trained personnel, 24/7/365 coverage, technology, translation services, and quality assurance processes.

An internally staffed hotline program – generally operated by the human resources, legal or ethics office – can offer an organization the ability to immediately respond to issues and ask detailed

follow-up questions. But the challenges associated with maintaining an internal hotline program are often overwhelming. From training intake specialists to providing the coverage needed, many organizations find that a professional hotline provider can offer these services for much less than it costs to implement internally.

No matter how an organization structures its hotline services – whether internally or through a third party – it is important to consider what happens after an incident is reported. Every organization needs established processes to manage the capture, dissemination and reporting of information that comes in through the hotline, online or open-door intake form.

Organizations also need strong investigation protocols, including guidance on when to investigate, how to select the person or group to conduct the investigation, the type of information to collect, and how to present the information in a report. Legal action is often the result of poorly conducted investigations. This is another area where a third-party provider can offer structure and expertise.

## **Who Should “Own” the Incident Management Program?**

The question of who should “own” the incident management program is often the subject of debate in the ethics and compliance community as well as within individual organizations. On one hand, human resources leaders argue that the majority of reports taken by incident management systems are HR related, so they should own the program.

However, the process is intended to be an independent reporting channel and is part of an effective ethics and compliance program in all the best practice

frameworks. Therefore, it is best practice for the chief compliance officer and the ethics and compliance team to manage the program, particularly in larger organizations with independent functions.

That said, planning and implementing the incident management program should be a collaborative and inclusive process that involves representation from several departments including legal, human resources, internal audit, security, risk management, loss prevention (if applicable) and IT. Stakeholders will need to partner to ensure the program is implemented smoothly and that all departments effectively get what they need from the program.

Further, the most robust programs have a “tiered” approach to receiving and managing incidents and reports. While the E&C group oversees their program, other departments such as HR should be able to record reports and separately see appropriate data from their group or division. At some higher level of the organization, however, someone should have the ability to access all data and run reports that combine statistics and data across the tiered departments for a holistic view of issues and incidents across the entire enterprise. When an organization has a separated, siloed incident management structure, the organization may miss patterns that could indicate serious problems as well as opportunities for additional training.



## Who Should Enter a Report Into the Incident Management System?

A variety of individuals and departments should have access to an incident management program to enter reports received from employees and others, including:

- Compliance
- HR
- Legal
- Security
- Environmental, Health and Safety
- Audit
- All Frontline Managers

## How Reports are Disseminated

One of the most important aspects of planning is deciding where to send information that is received through various reporting methods. Third-party hotline providers can help organizations develop a system of rules to determine what happens to information upon receipt of reports.

The goal is to set up a process that ensures complaints are not overlooked, mishandled or inadvertently dropped from the radar. Programs that are owned by the chief compliance officer should have all reports routed to them (and at least one other person within the department in case the CCO is unavailable) unless they are named in the report.

Once the report is received, the ethics and compliance department should use an established and agreed upon triage process for distributing reports to appropriate individuals and departments with a need to know or responsibility to conduct an investigation. A third-party incident management provider will be able to help the organization set up exclusions and alternate routings such as requests to route or copy reports of accounting irregularities to the Audit Committee of the board of directors.

As part of the planning process for an incident management system, the cross functional team should define a formal protocol for who is responsible for review and investigation of each type of report the organization may expect to receive. This planning is best done “in the abstract” and in advance of taking reports to minimize the emotions that may come with a specific report or allegation that may bias the approach. Below is a sample distribution structure that could be defined.

**Sample Report Distribution Structure:**

Issue	Potential Recipients
Employee Mistreatment	<ul style="list-style-type: none"><li>• Human Resources Officer</li><li>• Ethics Officer</li></ul>
Account Irregularities	<ul style="list-style-type: none"><li>• Internal Audit</li><li>• Loss Prevention</li><li>• Risk Management</li><li>• Ethics Officer</li></ul>
Workplace Violence	<ul style="list-style-type: none"><li>• Security</li><li>• Operations</li><li>• Legal</li><li>• Human Resources</li></ul>
Employee Theft	<ul style="list-style-type: none"><li>• Loss Prevention</li><li>• Human Resources</li></ul>

Depending on the organization’s structure, there may be other interested groups. For example, some organizations have a risk management or safety department that should receive reports of unsafe working conditions. Similarly, loss prevention should receive reports regarding internal theft, internal audit should get reports of vendor fraud and security should get reports of potential workplace violence. Clearly defined escalation policies are important processes for any program.

**Quality Metrics**

The planning process is also the time to define expected metrics on investigation completion time. While there are investigations that take longer due to complexity or legal ramifications, it is important to measure and report on case closure time and use this as a quality control performance indicator for the program.

**Escalation Criteria – Two Separate Approaches Needed**

All organizations should prepare two types of escalation policies: one for emergencies and one for identifying the types of reports that should be escalated to executive leadership and the board of directors.

**Escalation of emergency situations.** For initial report intake, the incident management implementation group must agree upon a list of critical topics that require immediate notification or escalation 24 hours a day by the third-party provider. These are separate from issues that will be delivered via standard dispatch protocols. It is important that management has a shared understanding of what is considered “high-risk” and how high-risk situations will be directed and escalated.

Emergency, high-risk situations that require immediate notification and escalation by the third-party hotline provider generally include:

- Threat of violence or physical harm to employees, customers or property
- Threat of business interruption
- Notice that a high-risk incident is expected to happen within the next 24-48 hours

The organization should implement a notification and escalation process for any emergency incidents that includes contacting key personnel at home



during nonbusiness hours. The process should be documented and include who the key personnel are, how they can be reached and steps for handling an emergency report. It is also important to identify at least three individuals to be contacted (in order) in case the first or second person are not reachable.

**Issue escalation to senior management and the board of directors.** Separate from emergency situations, organizations should have an escalation policy defining who needs to be notified of serious allegations requiring immediate investigation. All organizations should also have a written escalation policy developed with the board of directors describing the types of allegations that require immediate board notification.

Typically, the types of incidents that are covered in an escalation policy for the board include any allegations against a member of the executive leadership team and those that could cause serious harm to the reputation or finances of the organization. Best practice is notification within 24-48 hours. While this may already occur informally, it is important to have expectations in writing to support independence and to avoid the appearance of a conflict of interest and pressure to delay reporting.

## Special Considerations for Global Operations

Multinational organizations face special challenges when it comes to making incident reporting available to globally based employees. To ensure the incident management program is compliant outside of the United States, program leaders and the third-party hotline provider must understand the legislative and regulatory differences for all of the affected countries.

For instance, in the EU, the EU Whistleblower Protection Directive has created a sweeping change to whistleblowing laws and requirements across the continent. Perhaps the most consequential of the various requirements included in the Directive is the provision for entity-based reporting, which requires all legal entities within an organization to provide dedicated reporting channels and strictly control access to case data. Additionally, data protection laws governing transfers within and outside the EU continue to evolve, and have direct impact on how an incident management program must be implemented to ensure lawful data transfer.

It is critically important to the success and effectiveness of an international compliance program that incident management communications and awareness materials are reviewed for cultural sensitivity, nuances and country specific legal requirements. It is best practice, and potentially legally required, to involve managers and labor representatives from international locations in the development of all reporting-related communications in order to address cultural distinctions and any unique labor requirements. Discussing these issues during the early planning stages builds trust and helps garner support throughout the organization.



When planning for phone intake, the report intake interviewer should be able to conduct the interview in the caller's preferred language, using an interpreter if necessary. It is imperative that employees can report information in their preferred language, so they are as comfortable as possible during a potentially stressful or emotional conversation.

Offer equal accessibility for employees across the world. For example, global callers need to be able to place a toll-free call to reach the hotline. The organization cannot assume, however, that offering only a phone or only a web reporting option is sufficient for global support because this assumes all employees have access to reliable phone service or internet access. Many areas of the world continue to be challenged by poor and inconsistent phone and internet service, so having multiple reporting options available is critical. Consider providing an address for written mail as the last resort for employees.

When planning for a multinational incident management system, consult with the third-party service provider and local legal counsel for all the latest requirements that could affect the design and implementation of the program.

## Data Security and Retention

Keeping reported information secure is also a crucial aspect of the program's success. The incident management system provider or the organization's IT manager should be able to provide detailed information about the processes and safeguards in place to protect reported information and maintain its confidentiality.

Some of the questions an organization needs to address include:

- How vulnerable is the data to hackers? Is the system periodically audited for best practices in data protection?
- Is the data encrypted or otherwise secured while in transit and being stored?
- Have interviewers been trained about confidentiality and data protection?
- Have interviewers passed an extensive background check and signed a strict confidentiality agreement as part of the hiring process?

In certain jurisdictions, an organization may only retain records generated by the hotline or findings of an investigation for a specified period. Multinational organizations seeking to comply with guidelines of different countries should ensure their incident management system is set up to appropriately address the differences between jurisdictions and create policies and procedures to assist investigators and case managers in understanding necessary requirements. Top tier hotline and incident management providers are well positioned to assist companies with their compliance both from a domestic and international data security and privacy perspective.





# ■ Implement

## Promote Use of the Incident Management Program

Once an organization defines and agrees on a plan, it is time to implement it as well as drive awareness of the program with employees and relevant stakeholders.

Communication about the incident management program is a critical part of building and maintaining an ethical culture. Communication that encourages use of the program not only help detects issues, it can prevent them by reinforcing the organization's values and its commitment to operating ethically.

It is best practice to form an ethics communications team that will develop and implement hotline communication and awareness campaigns, which are essentially marketing campaigns that help the organization create, promote and maintain an ethical workplace and inspire a culture of speaking up.

As with any marketing campaign, the first step is to determine what actions you'd like to reinforce, and the key messages that will motivate these behaviors.

The next step is to understand the target audience (employees, suppliers or others) to determine how to effectively reach them. What are their demographics and psychographics? How and where do they best receive communications? What is their current attitude toward and perception of the organization and how it handles ethical issues?

Reporting potential misconduct is everyone's responsibility. Executive, mid-level, contract and support personnel alike may be aware of unethical behavior, so it's important to communicate clearly to everyone working with the organization about unacceptable behaviors.



Communications should clearly explain terms like "accounting irregularities" and "insider trading," which may not be clear to all employees. The key message to employees is "if you see something you think violates a policy or law, or just feels wrong – report it."

Finally, make sure the organization has an antiretaliation policy. Make it clear in communication materials that the organization will not tolerate retaliation in any form against anyone who reports issues; it is not only unacceptable, but also often illegal. If appropriate, use sanitized examples of how the organization swiftly handles allegations of retaliation.

## Use Multiple Delivery Methods for Awareness

Communication campaigns should be designed to educate target audiences and motivate them to report concerns. Adult learning theory is clear that people learn differently, so use a variety of delivery methods to ensure that the message is received.

Delivery methods could include posters in break rooms, emails, screen savers, virtual meetings, articles in employee newsletters, wallet cards, brochures and corporate intranet sites, and burst or micro-learning messages. Reinforce key messages at team-building meetings and other face-to-face events. It is also

important to consider the range of ages that make up your workforce and include mechanisms that are relevant across multiple generations

Many organizations take advantage of new communication campaigns to refresh their code of conduct, since they are getting employee attention and recommitting to ethical values. This is a good idea for many organizations with painfully old, out-of-date codes. In today's workplace, a code of conduct, along with an organization's incident management communications, needs to engage employees. The content should be easy to understand, written in a positive and inspiring tone and in language that is suitable for all employees.

**Key campaign messages should reinforce:**

Key messages	Provide examples of...
Behaviors that are expected	<ul style="list-style-type: none"><li>• Conduction business in a legal and ethical manner</li><li>• Reporting known or suspected wrongdoing</li><li>• Asking questions when not sure of the right decision or action</li></ul>
Behaviors the organization does not condone	<ul style="list-style-type: none"><li>• Illegal and/or unethical behavior</li></ul>
How to report witnessed or suspected misconduct	<ul style="list-style-type: none"><li>• Explain all of the avenues by which someone can report and how they operate</li></ul>
The defined process after making a report	<ul style="list-style-type: none"><li>• What employees can expect before, during and after they make a report</li><li>• What to do if employees believe they are experiencing retaliation</li></ul>

**Launching the Program**

Like any new initiative, an incident management program requires an organized and thoughtful launch to be successful. Begin with an employee announcement about the program that comes from the President or CEO. Showing support from top leadership establishes a tone from the top early in the process.

A program announcement or refresh should, at a minimum, include the following key messages:

- We all have a duty to act in line with our values and the law, and we all have a duty to raise concerns when we witness unethical or illegal conduct.
- Employees may report anonymously or confidentially.
- Retaliation is not permitted against any person who reports or who participates in an investigation. Retaliators will be disciplined up to and including termination.
- How people can report concerns, including a hotline number, online form address, and speaking directly with a manager.
- The process for what happens when a report is taken, i.e., who will take the report and who will investigate the report.
- What people can expect in terms of follow-up and resolution including the types of information that will and will not be provided when a matter is closed.

The campaign should not be a one and done. Ongoing reminders are needed in a variety of mechanisms and formats. Some research shows that people need to hear about something at least seven times to remember it, so include a reminder in all related training and ensure the information is easy to find on the organization's web page – not buried several levels down.

Ensure that all new employees receive the incident management program information as part of new hire training. Repeat this information several months later as new hires are taking in vast amounts of information during their first few days.

All managers should receive a guide and training during program implementation. The guide should give them details about the program, help them encourage employees to use the program, prepare them to handle questions and inform them how to document reports of issues that employees discuss with them directly via the leadership form. Be clear and specific about nonretaliation requirements and responsibilities.



## After the Call – Responding to Reports

### Sufficient Resources

Once an allegation is reported, it must be addressed, and when necessary, fully investigated. The organization should critically assess whether it has the available resources to support an investigative process or whether it should seek the services of an independent, third-party investigator. Delays in completion of investigations damages the reputation of the organization and the program. The 2021 NAVEX Hotline Benchmarking Report shows a continuing rise in the median number of days to close a report, with 22 percent of cases taking 100 or more days to close.

### Ongoing Communication with Anonymous Reporters

When working with an anonymous reporter, the goal is to capture complete and accurate information during the initial interview because there may never be another opportunity to ask additional questions. However, reporter anonymity does not negate the ability and responsibility for that person to follow up on his or her report or for the organization to ask additional questions.

Third-party hotline providers have a process for this. They offer the anonymous reporter a unique code correlating to their report and ask the person to call back after a pre-determined amount of time. This gives investigators a chance to review the information, determine any additional questions to ask the caller if they call back, and allows the reporter to call back while remaining anonymous.

Keep in mind that while the call-back process can enhance an investigation, roughly two-thirds of anonymous callers never call back, so the quality of every interview is critically important. Even if the person reporting provides their name, they may refuse to answer additional questions provided by the



organization, so having skilled interviewers available to draw out all critical facts during the initial interview is imperative. Some third-party solutions enable anonymous reporters to provide a follow-up email address—kept anonymous from the larger organization—that can be used for ongoing communication with the reporter without relying on a callback.

As part of the rollout and ongoing communications strategy, remind employees that if they choose to report anonymously, they are also encouraged to check back at the requested time to answer any additional questions and to check on the status of their concern.

## Investigating Allegations

As discussed in the PLAN section of this guide, all organizations should have established processes and procedures in place to investigate reports, and all investigators should be trained on the proper investigation techniques and expected documentation. Sufficient resources need to be available to completed timely reviews. As part of the planning process, organizations should put a formal investigation protocol in place that includes requirements for documentation of the process followed and the findings of the case.

A strong incident management program also tracks the quality and timeliness of completed investigations. Organizations should watch the metrics for specific investigating units and personnel. For example, watch for a certain team or person that consistently takes much longer to complete an investigation or has a consistently high or low substantiation rate. Follow up and take appropriate action for process deviations or inadequate skills.

## Tracking the Progress and Outcomes of Reports

It is best practice to use an incident management software solution to track the progress of cases that are submitted through the hotline and online form, as well as those that are disclosed to managers directly by employees and submitted via an open-door process. In addition, when other departments receiving reports such as HR or security enter their reports into the same system (even if tiered for limited access) the overall database will reflect a holistic picture of what is happening in the organization, and reporting to the board and leadership is more robust.

A sophisticated incident management solution allows an organization to document every report, as well as the actions taken to investigate each allegation, the final disposition of the investigation and the nature of any disciplinary or other resulting corrective action. This documentation may be required in the event of litigation and can be used to demonstrate consistency in approach and actions taken. Providing an established system for documenting investigative activities is another area where a third-party hotline provider helps organizations increase their defensibility.



## Recognition and Information Publication

There has been much discussion over the last 20 years about whether reporters should be recognized and/or rewarded for raising issues. Some organizations have done this successfully and believe this type of recognition has had a positive impact on culture and the reporting environment. Others believe this practice is either not needed because reporting is an expectation of all employees or worry that highlighting specific individuals could backfire on the person or the organization. This decision is one that will be unique to the organization and is worthy of some discussion of the pros and cons.

Regardless of whether individuals are recognized, it is most important to regularly publish some information about the types of reports received and the types of actions the organization has taken as a result. Legal departments have varying levels of comfort with the notion of publicizing hotline statistics, but organizations that do this generally have positive experiences. The level of detail will be unique to each organization but letting employees know that others have trusted the system and appropriate actions have been taken will help build confidence in the incident management program. Sanitized cases are always of interest to employees. This is one topic where challenging the legal arguments against publication is an important discussion.



## When The Incident Management Program is 'Stuck in Neutral'

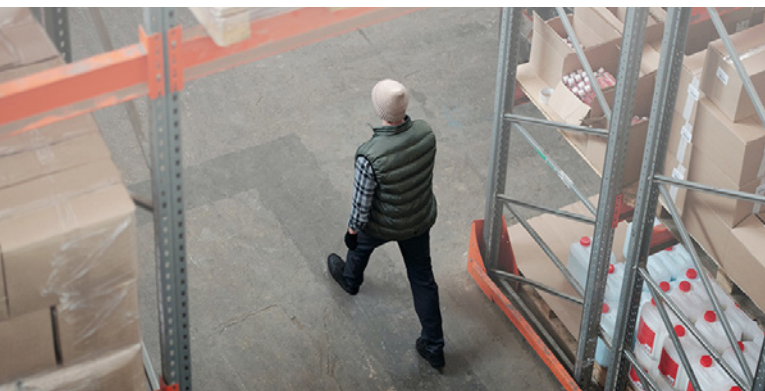
Some compliance officers feel their ethics and compliance programs cannot sustain traction regardless of how much communication they generate to promote awareness.

For example, one compliance officer was frustrated by the findings from a recent third-party assessment which revealed that, for the third year in a row, their hotline/helpline call volume was significantly below industry benchmarks.

Another was surprised by the number of potential conflicts of interest that were surfacing among sales personnel, despite their new code of conduct and updated policies that were published last year.

A third confided they could not seem to break through to front-line managers who continued to offer only tepid support for training initiatives.

In each case these were experienced compliance officers whose programs had all the expected basic and required elements. But somehow, their programs were not adding up to an effective whole. As a result, persistent problems continued.



## Root Cause Diagnosis: Program Awareness and Communications Missing the Mark

Diving deeper into these challenges, a common root cause began to emerge. In every case, information that was being provided through communications, training and awareness efforts, was missing the mark.

For example:

- The low helpline call volume described by the first compliance officer could be traced to employees not being aware of how the helpline process works. Employees knew that there was a hotline or helpline, but the call-in and follow-up process was a mystery. This added to their fears of the helpline and became an additional – and unnecessary – hurdle.
- The second compliance officer's spike in conflicts of interest cases was rooted in a failure to earn attention amidst an avalanche of emails and priorities that were burying the sales team.
- And the third compliance officer's front-line managers simply did not have the time to sort through long and complex training materials and "ethics toolboxes" – no matter how well they were constructed. What was needed was a just-in-time system they could use to select ethics messages when they would do the most good to support their employees.

## Solution: Delivering the Right Message to the Right Audience at the Right Time

Each of these programs needed to improve in the essential task of delivering the right message to the right audience at the right time. While this may seem obvious, it is surprising how often organization have

not taken the time to develop a compliance awareness plan for their ethics and compliance program. To create a best practice plan, consider the best ways to:

**Prioritize messages.** What messages need to be delivered and to whom? Targeting the right message to the right audience is critical. In our above example, the sales team did not need to receive every ethics message on every topic. Targeted messaging about gifts, entertainment and conflicts would be far more effective.

**Choose the right timing.** Coordinate the ethics and compliance message with other corporate initiatives. Avoid the end-of-the-month crunch times when stress is high, and time is short.

**Diversify communications and awareness formats.** Not everyone will respond to the same media. Posters are good for some and intranets for others. Emails may be effective, but not when they are lost in a backlogged inbox or are too easily deleted. For people inundated with emails, a different approach may be necessary to cut through the electronic clutter.

## Awareness and Communications Planning and Execution Essential for Program Success

The key to success is thoughtful and balanced awareness and communications planning. When so much time and so many resources are put into designing and creating a helpline, a new code of conduct or a training program, compliance professionals must avoid letting the effort fail to hit the mark due to a failure to plan how, when and to whom the information is going to be shared.

# ■ Measure

## Monitor and Improve Program Effectiveness

An incident management program is dynamic. Reporting activity will naturally ebb and flow, and each organization will develop its own standard. The introduction (or elimination) of a training program, having the CEO and top management speak with renewed emphasis on the organization's commitment to ethical behavior, or even a lapse in written communications about ethics – and many other factors – can contribute to the number and pattern of reports that an organization receives at any given time.

The best reporting programs take advantage of available data and use it to gauge the effectiveness of campaigns, assess the need for additional training, track trends and evaluate the overall health of the organizational culture.



A third-party incident management vendor provides access to reporting tools that help organizations detect problems, analyze trends and manage the program. Incident management tools provide both a high-level summary as well as detailed information when filtered by incident type, volume, time frame and location.

The formatting and display of the data is important; a graphical format can make it easier to interpret the data and make educated business decisions. For organizations that use incident management tools, reporting should include details about the status, volume and resolution of investigations. Reporting allows organizations to look for “hot spots.”

For example:

- Is there a division that seems to have more issues than others? If so, is additional management attention needed to review the culture or leadership style in that division?
- Are there additional training needs?
- Is there an investigator or department whose number of past-due cases is consistently high? There may be a need to evaluate the investigator's caseload or skills.
- Is there one location where very few calls are made? Perhaps this location requires better or more hotline communications. Or is this a location with a higher level of fear of retaliation?

## Benefits of Monitoring the Incident Management Program

Monitoring the incident management program is an important process that allows an organization to track, adjust, and improve – as well as ultimately predict reporting activity. Following are the top reasons organizations should carefully and consistently monitor the incident management program.

**Ensure the program is up-to-date.** Organizations must track regulatory changes and whether those changes impact the operation of the program. Do changes in whistleblower or data privacy laws in geographies of operation require new language on the hotline greetings? Has a new regulation caused a spike in hotline activity?



### Link reporting trends to training and awareness

**needs.** Ongoing monitoring of reporting data allows and organization to identify where additional training and awareness are needed. Conversely, track changes in activity that happen around awareness campaigns, communications and training. For example, when antibribery training is delivered, is there a spike in reports or questions for all incidents or just bribery related incidents?

### Be prepared for predictable changes.

Many organizations have predictable changes in reporting activity during times of the year when employees are asked to attest to policies or take training. An example of this is during gift-giving season. Employees will often see an increase in program activity related to gifts and entertainment-related reports or questions, making this a good time to deliver targeted training to prevent issues from arising.

**Track employee engagement.** Many companies monitor reporting activity after a significant organizational change, such as new senior leadership or organizational restructuring. This gives leaders a sense of how employees are faring after a major transition and whether specific action needs to be taken for example, to prevent burnout and keep the culture strong.

## Measuring Program Effectiveness With Benchmarking

Reporting on program effectiveness is an important tool in determining the level of resources needed to support the program. To evaluate the effectiveness of incident management programs, compliance officers and their boards typically turn to benchmarking against the activity of similar organizations. Are other organizations seeing the same rate of anonymous reports? On average, what percentage of employees report through the hotline within a certain industry? What incident types comprise the highest number of reports industry-wide?

Benchmarking provides organizations with the metrics to determine if reporting activity is considered high (or low) within the industry. This knowledge can drive the need for change within a reporting program, suggest the need for new initiatives or reinforce the effectiveness of ones that are already in place.

NAVEX annually analyzes data from anonymized reports to provide the deepest reporting benchmark data in the world. It is the industry's most comprehensive intake and incident management benchmark report representing:

- 10,000 NAVEX customers
- 57 million employees globally
- Over 1.25 million reports each year
- Data from over 120 countries
- Intake methods including web, hotline, open-door, email and mail
- Data covering 31 industries

Get a copy of the most recent Hotline and Incident Management Benchmark Report [here](#).

## ■ Conclusion

A growing body of research continues to confirm the benefits of having an ethical business culture and its impact on organizational success. Giving employees a variety of ways to report misconduct and violations of policy – including hotline, web reporting and open-door intake – reinforces the organization's commitment to ethical business practices.

NAVEX recommends using software (like EthicsPoint® Incident Management) for a consistent approach to data collection and enterprise-wide tools to manage multiple reporting programs. This enables users to easily identify actionable trends, mitigate risk, and manage a successful incident management program anywhere in the world, while being audit-ready and current with the everchanging business environment.

A strong incident management system is not only critical to engaging employees and building trust within an organization – it is a vital component to protecting an organization's people, reputation and bottom line.



# About NAVEX's Incident Management Solutions

NAVEX One, NAVEX's smart integrated risk and compliance platform, automates the management of all types of risk, leverages data and provides actionable insights.

The NAVEX Ethics and Compliance solution is an automated suite of products designed to meet all ethics and compliance needs and solve regulatory and people-based risks.

## Hotline and Incident Management

The ethics hotline provider trusted by thousands of customers around the world, our employee hotlines help staff, customers, suppliers and other stakeholders to report potential ethics and compliance issues quickly and easily.

EthicsPoint®, NAVEX's hotline and incident management software, helps organizations demonstrate their commitment to operate ethically. It captures and investigates ethics and compliance reports from across the organization in a centralized database.

This way, organizations can apply the knowledge gained from their incident management program to enhance training programs, modify policies or revise their code of conduct.

## Awareness Solutions

Promote awareness of key E&C program components, including hotline and key training messages, with NAVEX's proven awareness materials.

To learn more about our EthicsPoint Incident Management software or to schedule a demonstration of any of our solutions, visit [www.navex.com](http://www.navex.com).

For additional information and downloadable resources, visit the [NAVEX Resource Center](#).



NAVEX is the recognized leader in risk and compliance management software and services, empowering thousands of customers around the world to manage and mitigate risks with confidence. NAVEX's mission is to help customers promote ethical, inclusive workplace cultures, protect their brands and preserve the environment through sustainable business practices.

For more information, visit [NAVEX.com](https://navex.com) and our [blog](#). Follow us on [Twitter](#) and [LinkedIn](#).



#### AMERICAS

5500 Meadows Road, Suite 500  
Lake Oswego, OR 97035  
United States of America  
[info@navex.com](mailto:info@navex.com)  
[www.navex.com](https://www.navex.com)  
+1(866) 297 0224

#### EMEA + APAC

4th Floor, Vantage London  
Great West Road  
Brentford, TW8 9AG  
United Kingdom  
[info@navex.com](mailto:info@navex.com)  
[www.navex.com](https://www.navex.com)  
+44 (0) 20 8939 1650