CASE BY CASE:
CENTRALIZING & STANDARDIZING INCIDENT INTAKE, INVESTIGATION AND MANAGEMENT
Allegations of misconduct can be reported via one of three primary reporting channels:

1 **TELEPHONE HOTLINE**
   Reports are filed via external call center.

2 **WEB INTAKE FORM**
   Employees make reports online.

3 **PROXY**
   Designated proxies (from compliance, legal or HR, for example) enter whistleblowing reports on behalf of reporting parties that may have been received directly by email, phone, SMS, etc.

Regardless of the channel through which an incident is received, best practice is to have them recorded and managed in a single, centralized location for accessibility, comprehensive reporting capabilities and to ensure consistent investigation and response procedures across all incident types and reporting channels. Call center agents and proxies should not lead the reporting party in any way and enter information exactly as reported.
GUIDED VS. SIMPLE INTAKE

There are two types of intake questionnaires based on two different philosophies of who should classify an incident type: the employee making the report or an administrator.

GUIDED INTAKE

Employees submitting issues classify the issue type, then answer incident-specific questions. The issue is routed according to their classification and your routing rules.

SIMPLE INTAKE

Reporters are asked first to explain the incident, then provide relevant details. Once the report’s submitted, administrators categorize the issue type based on the information provided and it’s routed accordingly.

As Guided Intake is the more widely used method, we’ll cover it here. Whether a report is made over the phone, online or via proxy, the steps below represent the type of information to gather, in recommended order.

1. Select the location and where the incident occurred.
2. Acknowledge the terms and conditions, which usually include a notification that the intake channel is not an emergency service.
3. Select the issue category and a series of related questions.
4. Describe what happened and provide information about the involved parties (subject, witnesses or victims).
5. Provide the date and location where the issue occurred.
6. Upload any files, photos or documents to support the allegation. If making a report via the call center, reporters can access their report and submit relevant files online.
7. Provide your information and anonymity preferences.
8. Review and verify report accuracy.
9. Create a password and security question that will let you access your case at a later date.
10. Receive and record the case number.
INTAKE

1 ROOT CAUSE
Track employee intent and identify underlying behaviors or conditions that contributed to the misconduct. When you aggregate that data, you can identify common root causes of behavior as well as patterns that identify what employee populations are more likely to engage in violations, enabling you to take a more targeted and proactive approach to risk management.

2 MULTIPLE ALLEGATIONS
You should be able to identify, track and manage multiple allegation types within a single incident. This not only reduces administrative burden on the employees making and managing reports, but it allows you to better understand everything that happened within a single incident and what types of misconduct are commonly related so that you can tailor your controls accordingly.

3 OPEN COMMUNICATION
Q&A functionality can help employees get clarity on potential gray areas, open the lines of communication and reduce extraneous incident reports. Once done filing a report, each reporter should have a secure way to ask questions, check on the status of their issue or provide additional details or evidence—even anonymously.

KEY CONSIDERATIONS FOR INTAKE CHANNELS

4 ANONYMITY
It’s important to protect the identities of the employees raising concerns as well as the subjects of their reports by offering levels of reporting party anonymity that may include:
- Remaining known to both the organization and third-party hotline provider;
- Known to the provider but anonymous to the organization; and
- Completely anonymous to the organization and third-party provider.

Case access controls, routing capabilities and escalation functionality can also ensure that security and confidentiality are consistently maintained; the risk of retaliation reduced; and that information can only be accessed by those who need to know and are not named in a report. Should anything go to investigation/litigation, the access or restriction of access to the report should also be documented to protect the organization and show that the report was properly managed.
THE PROCESS OF INVESTIGATION

It’s essential to develop a standard process for planning, conducting and reporting on the findings of internal investigations. Without clear and documented investigation protocol, your actions might not stand up in court or may be ineffective, inefficient and/or disruptive to your organization. What’s more, consistent investigations conducted in the same way can reveal important insights that help you prevent problems from happening again, instead of just reacting to incidents. Your case management system can and should facilitate this investigation process.
1. ASSESS THE ISSUE

What—if any—potential violations have taken place? What company policies or laws may have been broken? What version of that policy was in effect at the time the incident occurred?

Who should be notified?

If an investigation is required, will you handle it in-house or enlist outside investigators?

2. PLAN & DEFINE OBJECTIVES

What are you trying to achieve and what will it take to get there?

What’s the standard of proof you will need for each investigation’s findings?

What information will you need to meet your objectives (who, what, when, where, how, why)?

Which members of your team will be involved with each investigation?

Who will actually conduct the investigation?

Who are the decision-makers who have the authority to make the final call on any disciplinary action?

3. GATHER THE INFORMATION

You may leverage a variety of investigation methods, including interviews, research and audit, physical or electronic surveillance, forensic analysis or undercover research.

Your case management system should allow you to:

• Record all tasks and activities, who performed them and when and where they took place.
• Record all evidence, including digital files or a description of physical evidence and its location.
• Log descriptive notes for all tasks or evidence, such as a summary of an interview.
• Identify all parties involved, including reporters, witnesses, affected parties, subjects, interviewees and investigators.
• Log all email communications related to the investigation.
• Provide limited access for managers or other non-investigators who need to check on the investigation status.

4. VERIFY AND ANALYZE

Conduct interviews with the subjects in a neutral location and always have a third person in the room to act as a witness.

Start the interview by explaining how you learned of the allegation and describing all the methods you used to investigate the incident. Then, let the employee know that you’ve reached a conclusion and that this is his or her chance to explain the other side of the story.

Your goal is not just to resolve this case, but to prevent similar incidents from happening in the future. To do this, you should get the person to:

• Admit to the offense
• Tell you how and why they did it
• Find out who else was involved or if other offenses occurred

Record in your case management system that the interview took place, and note when and where it occurred and who was present. Also provide a summary or notes that describe the details of the interview.
5. PRESENT RESULTS AND MAKE A DECISION

If you’ve been logging your investigative activity in a case management system, it should be relatively easy to compile the information needed for a report. The format you choose for this report will depend on your company’s individual needs, but in general should include:

• An executive summary outlining the basic facts of the investigation, including the original allegations, the outcome of the fact-finding process (i.e., whether a violation occurred) and who was involved with the offense.

• A detailed account of the investigation that describes all the methods you used, the evidence you uncovered and which claims you’ve substantiated and which you haven’t.

• A list of evidence supporting your conclusions, including interview summaries or other corroborating documents.

• Copies of the signed admissions of the people involved with the offense.

• A final summary reiterating the investigation’s findings of fact, including which policies or laws were violated and what controls were in place to prevent, uncover and address these violations.

The investigation report should stop short of making recommendations for disciplinary action. Not only is that the decision-making team’s job, but you could also expose your company to risk if the decision-making team doesn’t follow up on those recommendations for any reason.

6. DETERMINE DISCIPLINARY AND CORRECTIVE ACTION

The decision-making team uses the findings in the investigation report to determine an appropriate response to the incident, which is documented in the investigation file along with a note when the disciplinary or corrective action actually takes place. You can create a follow-up plan to ensure any corrective actions take place.

7. CLOSE THE LOOP

Always circle back to impacted employees after an investigation concludes to let them know you’ve resolved the issue. It’ll increase their perception and confidence in organizational justice and transparency.

Finally, it’s important to seize the opportunity to find and correct any root causes of bad behavior. Whether operational problems like weak controls or cultural issues like management pressure or misaligned performance incentives, understanding the drivers and influencers of bad behavior better enables you to prevent it from occurring in the first place.
LEVERAGING YOUR CASE MANAGER

When a reporting party submits a new issue, all individuals that are configured to access that issue are notified. In addition to the investigation process above, you may take the following steps to manage the case within your case management platform:

• Review the summary to quickly understand the allegation types, the reporter’s relationship to your organization, where and when it occurred, how and when it was reported and the involved parties.

• Update issue details like the status, issue owner(s) and severity level.

• Link the issue to any related issues or organizational policies that may have been violated.

• Add or deny access to the issue.

• Update your notification preferences for individual issues and/or investigations.

• Manage the issue by following the investigation steps outlined above, in addition to communicating with the reporting party and internal team members and creating and managing tasks.

• Update the status, resolution type and any supporting details/notes once the issue has been resolved.
In addition to providing an affirmative defense in the event of a breakdown, case reporting and analytics provide interactivity, segmentation flexibility and rich visualizations that enable compliance executives and investigators to find patterns, locate correlations and ultimately determine causality. As a result, you’re armed with the information you need to ensure consistent investigations and responses and help you derive real knowledge about the motivators and contributors that drive employee actions.
Convercent’s risk-based global compliance solution enables the design, implementation and measurement of an effective compliance program. Delivering an intuitive user experience with actionable executive reporting, Convercent integrates the management of corporate compliance risks, cases, disclosures, training and policies. With hundreds of customers in more than 130 countries—including Philip Morris International, CH2M Hill and Under Armour—Convercent’s award-winning GRC solution safeguards the financial and reputational health of your company. Backed by Azure Capital, Sapphire Ventures (formerly SAP Ventures), Mantucket Capital and Rho Capital Partners, and based in Denver, Colorado, Convercent will revolutionize your company’s compliance program.

Visit us at www.convercent.com