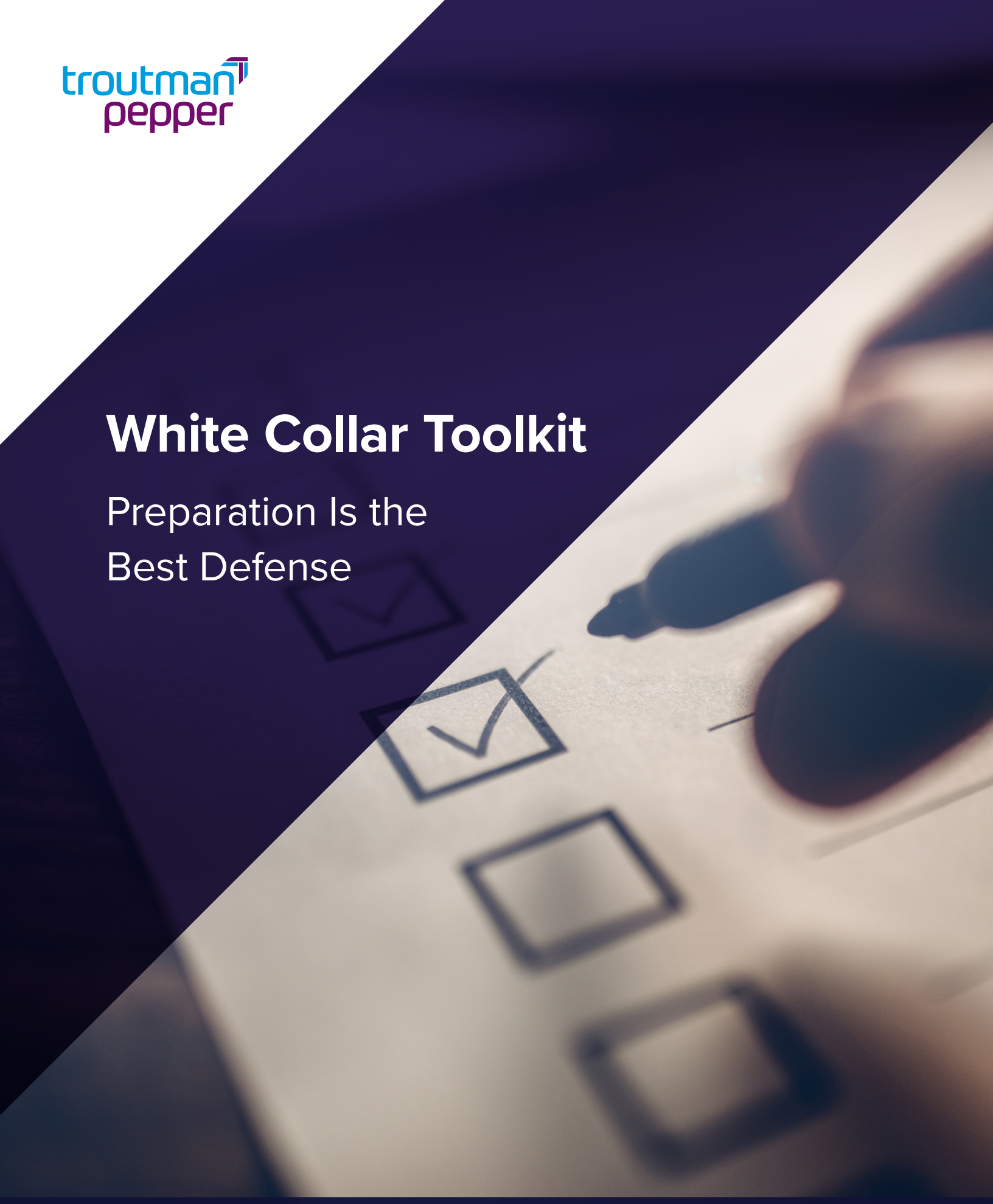
troutman pepper

White Collar Toolkit

Preparation Is the Best Defense



troutman.com

When Things Go Wrong

A Compliance How-To Guide

The right response to the discovery of a potential issue — either resulting from an internal report or government action — should include the necessary correction, mitigation, and implementation of a compliance program to prevent a future reoccurrence. Any existing compliance program must be reviewed and updated to ensure its effectiveness.

A Compliance Program Is Essential

- The U.S. Department of Justice (DOJ), the Securities and Exchange Commission (SEC), and other federal enforcement agencies place a premium on compliance.
    - Prosecutors consider the adequacy and effectiveness of a company's program when determining whether to bring criminal charges.
    - A robust compliance program may contribute to cooperation credit or to a mitigating factor in a damages analysis.
- An effective compliance program works and plays a critical role in preventing and rooting out criminal conduct. It will also help prevent business and reputational harm.
- A well-tailored compliance program is proactive, enabling better results than solely defensive measures.

A Compliance Program Must Be Thorough

Stakeholders must ensure that comprehensive compliance programs are developed and implemented.

- **Customization**

  A company should tailor its compliance program to its specific business and industry.
    - Cookie-cutter or "canned" compliance programs pulled from a search engine result or copied from another business are inadequate.
    - A company must think critically about their sources of compliance risk, why they exist, and what can be done to mitigate and monitor them. A company's size, locations, structure, business practices, and industry will impact its analysis.
        - This includes traditional business risks and developing risks introduced by new business technologies, such as the company's approach to employee use of personal devices and "off channel" messaging platforms, as well as the preservation of other communication, collaboration, and messaging platforms used by employees.
    - The mere existence of a program is not enough: companies must have processes and dedicated resources to ensure their programs are implemented. Essential questions for

consideration include:

- Does senior and middle management incorporate compliance into the company's culture? The "tone at the top" and middle are equally important.
- Is compliance incorporated into the evaluation and compensation processes?
- Are investigations independent, thorough, and prompt? Is misconduct met with appropriate consequences?

◦ Document the program's development, use, and whether it is designed to meet the company's needs.

- **Third-Party Management**

  A company must focus on compliance before, during, and after engagement.

- **Compliance Updates**

  A proper corporate compliance program is subject to periodic evaluation and improvement.

  ◦ An instance of past misconduct is a sign that a compliance program should be updated.

  ◦ A company should conduct root-cause analysis designed to identify the gaps in the compliance process.

  ◦ A company should undertake proactive measures to identify areas in need of improvement *before* misconduct occurs, including periodic internal audits of control and tracking systems, and engaging with employees to identify areas of weakness.

  ◦ An evaluation should be data-driven and tailored appropriately to higher-risk activities. Factors to consider include risk assessments, audits, and prior investigations.

  ◦ Companies should implement a schedule for periodic reviews of compliance training, policies, and controls to ensure that the program is not stale and aligns with the most current risks facing the company and the industry.

A Compliance Program Must Be Effective

Stakeholders must ensure their program works and addresses their particular compliance concerns.

- **Customized Training**

  Implementing a generalized training program will fail to provide necessary information and strategies. Training must be tailored to maximize its effectiveness.

  ◦ The audience determines the substance and method of delivery of training sessions:

  - New employees should receive a basic, high-level compliance training prior to being provided with more thorough sessions on the details of the program.
  - Existing, long-term employees would likely benefit from "refresher" training sessions that focus on recent compliance events or newly revised compliance policies.

  ◦ The substance of training on certain compliance topics should be varied based on the employees' levels within the organization. Employees in supervisory roles, for example, must be provided with the tools to investigate and address internal reports of potential compliance issues.

  ◦ Employees should be required to demonstrate their comprehension through on-the-job simulations.

- **Importance of Internal Reporting**

  Internal compliance reporting should be actively encouraged to avoid creating whistleblowers.

  - Implement multiple mechanisms that allow employees to report compliance violations, including one or more methods for anonymous reporting. Examples include a hotline, a lockbox for hardcopies, or an email account or portal that anonymizes the sender's identifying information.
  - Implement a system to quickly conduct thorough internal investigations of all complaints received, including reviewing relevant documents and interviewing potential witnesses.
  - Implement safeguards to prevent retaliation, including strict policies that forbid retaliation against whistleblowers. This may include placing employees accused of misconduct on administrative leave pending the completion of an investigation, particularly employees in positions of authority.

- **Punishments and Rewards**

  Stakeholders should use incentives and disciplinary action to drive compliance-promoting behavior and prevent compliance violations.

  - Implement disciplinary policies that empower leaders to create deterrents that maximize their impact. In at least certain circumstances, ensure that the company also has flexibility to determine the appropriateness of a companywide communication regarding the incident.
  - Incentivize employees to prioritize compliance, including, for example, linking a compliance metric to employee compensation, bonuses, performance reviews, or career advancement. Examples include requiring a clean compliance record; and completing compliance training for the eligibility of an annual bonus or promotion. Document the impact of these factors on decisions, such as discretionary raises, bonuses, or promotions.
  - Hold wrongdoers accountable by developing tailored policies for clawing back compensation and bonuses.

The Bottom Line

Robust, well-tailored, and adequately resourced compliance programs are vital, and companies should resist the temptation to take shortcuts. It is important that companies act quickly when a potential issue arises to understand the problem and how it occurred, while incorporating lessons learned to strengthen the compliance program moving forward. The process must include thoroughly developing, implementing, and revising compliance programs to ensure that they address a company's unique concerns and risks.

Leadership in the Crosshairs

A Guide to Evaluating Allegations of Misconduct Against Executives and Board Members

Allegations that corporate executives, senior management, or board members have committed misconduct expose a company to civil and criminal liability and — depending on their nature and scope — have the potential for catastrophic reputational harm. Addressing the situation requires immediate attention and decisive action.

It is important to remember that in-house counsel does *not* represent the alleged wrongdoer.

- In-house counsel represents the company — not its employees, executives, or board members in their individual capacities.
- In-house counsel must clearly inform the accused individual(s) that they do not represent them.
- In-house counsel must inform the individual of the privilege implications. Specifically, in-house counsel is not obligated to keep confidential any information the individual may share; and, to the extent in-house counsel receives any privileged information from the individual, that privilege belongs to the company and may be waived by the company at its discretion.

The legal department may, and in many cases should, assist the individual in retaining an attorney.

- Individual(s) may need to retain an attorney if their interests conflict with the company's interests.
- The company may assist the individual in selecting an attorney — for example, by providing a slate of qualified candidates. However, the individual must make the decision.
- The company's indemnification and advancement policies and the individual's employment contract must be reviewed to determine whether, and to what extent, it will cover the individual's legal expenses.

The company must determine the nature and scope of the alleged misconduct.

- It is important to consider whether the individual's actions were (1) within the scope of the individual's duties, and (2) intended, at least in part, to benefit the company.
- The company must determine whether it should provide notice under their Directors and Officers insurance, or other potentially applicable insurance policies.

- The company's independent internal investigation into the alleged misconduct must isolate the root cause, examine internal controls, and develop an effective remediation plan.
- When the government inquiry targets a C-suite executive or a member of senior management, the board of directors (the Board) should engage independent outside counsel to oversee the investigation to ensure impartiality and avoid the appearance of impropriety.
- The Board should convene a special committee of independent directors if a board member is implicated in the alleged misconduct. Independent outside counsel should report to the special committee.

Follow established investigatory processes and practices.

- The company should investigate its executives and board members just as it would any other employee. Leadership should not be given special treatment, but the nature and subject of the investigation may make it necessary to deviate from standard policies and procedures. For example, allegations against the company's general counsel may require outside counsel to report directly to the chief executive officer and/or the Board.
- Depending on the nature of the alleged misconduct, it may be appropriate to collect documents and communications pertaining to the accused executive that are within the company's possession, custody, or control without the executive's express knowledge and potentially even before they are made aware of the investigation
- Refer to our accompanying internal investigations guide for additional information on creating an effective internal investigations process.

Scope the investigation to maximize cooperation credit from the government.

- The interests of the company and the individual may diverge at any point during an investigation, and under certain circumstances, the company may be held criminally or civilly liable for the individual's illegal conduct.
- Prosecutors often offer "cooperation credit" (*i.e.*, a lesser sanction) to companies that have assisted the prosecution in its investigation.
- The government will want to know which individual(s) at the company were involved in and/or responsible for the misconduct. For example, to receive cooperation credit from the U.S. Department of Justice (DOJ), a company must disclose "all relevant, non-privileged facts about individual misconduct" regardless of the individuals' role or position within the company. Similarly, "the need for companies to share information on individual wrongdoers in order to receive cooperation credit… has long been a central tenet of cooperation with the SEC."
- To receive *maximum* cooperation credit from the government, a company must make these disclosures and produce all relevant evidence on a *timely* basis.
- When assessing a company's eligibility for full cooperation credit, the DOJ will consider whether the "company promptly notified prosecutors of particularly relevant information once it was discovered, or if the company instead delayed disclosure in a manner that inhibited the government's investigation."

- The company should structure its internal investigation — breadth and depth — to maximize its efficacy and allow for scaling up or down as the facts unfold.

Develop a public relations strategy to mitigate reputational harm.

- Depending on the nature and scope of the alleged misconduct, a company should convene a team that includes at least one communications professional to vet all public statements about the matter.
- In addition to protecting the company's reputation, this team should ensure the consistency of all external communications — including statements to the press, disclosures to investors, regulatory filings, and representations to government investigators.

When the Government Asks Questions

A Guide to Responding to Government Inquiries

In today's highly regulated environment, businesses in any industry sector should be prepared to respond to a government inquiry. While each situation is unique, an organization's response to the initial government contact often sets the tone for how an investigation unfolds. It may also materially impact the ability to favorably resolve regulatory or related public relations threats.

These best practices should be followed by companies involved with government inquiries:

Educate yourself and your employees about investigative tactics.

- Questions from law enforcement may be presented via telephone, e-mail, letter, or virtually anywhere in person.
- Subpoenas and Civil Investigative Demands (CIDs) are also commonly used to elicit information and statements from unprepared recipients.
- Establish clear points of contact and lines of communication to ensure that surprise and routine initial contacts with law enforcement are addressed promptly and properly.

Triage written requests for information.

- **Memorialize service**
  Carefully record the date and time of service of a subpoena or CID for future reference. A prompt acknowledgment to the agent or prosecutor and early assurance of your intent to keep the lines of communication open can change the course of an investigation.
- **Understand the scope**
  A subpoena or CID does not entitle an agent to search your files or devices.
- **Know your regulators**
  Determine the identity of the issuer and whether the issues are administrative, civil, criminal, or all the above. The mechanism is equally essential to this analysis —CIDs are a powerful pre-litigation tool, while a grand jury subpoena means that a criminal investigation is underway.
- **Consult counsel and create your response plan**
  Subpoenas and CIDs rarely compel the immediate production of documents, and subpoenas for testimony may be negotiated into an informal interview, attorney proffer, or witness proffer instead of a stressful appearance. Respond only after carefully reviewing the requests with an attorney.

Preserve records and develop an action plan.

- Send a document preservation notice to people who may have relevant information to avoid all appearances of obstruction of justice. Be thoughtful in the messaging: such notices can often generate office speculation or gossip.
- Work quickly and closely with your IT, HR and Records departments to suspend any regular data disposition procedures, ensure the separation of custodians' information is maintained, and collect potentially relevant documents and communications. Engage an electronic discovery provider to perform the collections if you do not have the necessary in-house expertise.
- Assess whether an internal investigation is necessary or desirable with the assistance of an attorney. Depending upon the subject matter, a parallel internal investigation may help to ensure that the illegal conduct or other wrongdoing has stopped. An internal investigation may also counter any incomplete or inaccurate assertions made by the government, and allow you to implement measures to promptly mitigate liability.
- Where a subpoena or CID requests substantial document discovery, begin a dialogue with the agent or prosecutor about production timing, scope, and format, as well as privilege logging, with the goal of negotiating reasonable search criteria, sufficient time to perform a comprehensive attorney review, and acceptance of a less burdensome categorical or objective metadata privilege log.

Be prepared for interviews.

- ### Tell the truth

  It is a felony offense to make a materially false statement in response to questioning by the government, regardless of the context. The government does not have an "off-the-record" interview or conversation. Agents are not required in many jurisdictions to ask permission nor to inform you about recording a conversation with you.

- ### Verify credentials

  Request — and verify — the interviewer's agency, badge or ID number, and phone number before speaking with them.

- ### Understand your right to remain silent

  There is no legal mechanism for an agent to compel an interview. Without a subpoena, and regardless of what the agent may say, the choice to respond belongs to the interviewee.

- ### Collect intelligence

  Request information about the nature and subject matter of the investigation and for records or other information that can or should be reviewed in advance. Ask whether you are a witness, subject, or target of the investigation.

- ### Consult counsel

  Ensure that employees understand their right to consult with an attorney and for the attorney to be present for any future interactions with the government. At the very least, have a third-party witness participate. Company counsel should be notified in advance and permitted to attend if the interview will be about the interviewee's work for your company.

- ### Be alert to coercion

  It is improper for an agent to use the threat of a subpoena or search warrant to coerce statements from employees. Advise the interviewee that they have the right to terminate any conversation and/or schedule an interview with an attorney in attendance.

What to Do When the Whistle Blows

A Reference Guide for Investigating Internal Complaints

All companies inevitably face complaints that allege improper, unethical, or illegal conduct. The best-run companies welcome those complaints because it provides an opportunity to investigate the allegation, determine whether wrongdoing occurred, and (if necessary) fix the problem. Oftentimes, how companies respond to complaints becomes just as important as the underlying alleged conduct — the Department of Justice, for example, may take a more lenient approach to companies that promptly investigate and remediate misconduct. Still, that leniency will disappear if companies try to delay or minimize an investigation.

As a result, it is imperative that companies follow these best practices when the whistle blows:

Take all complaints seriously.

- Whether reported through internal channels or offhand in a social media post, even informal or vague complaints can lead to investigations of consequence.
- Experienced employees should evaluate all complaints to determine whether an investigation is warranted, and if so, who should conduct the investigation.
- And if the complaint alleges ongoing unlawful activity, take steps to ensure that the activity stops immediately.

Do not investigate the whistleblower.

- The company must, in policy and practice, have zero tolerance for retaliation against whistleblowers.
- Investigate the allegations, not the whistleblower. If the whistleblower is anonymous, do ***not*** try to determine the whistleblower's identity.
- While the whistleblower's motivations or credibility may become important to the investigation, the investigation must first and foremost focus on whether the allegations are true.

Make an investigation plan and know that it will change.

- Set the investigation's scope by defining the issues to be investigated and identifying the relevant people, documents, and time period.
- Identify who needs to know about the investigation and when. Investigations also spur office gossip, and you may not want potential witnesses to know an investigation is pending until you have the opportunity to preserve evidence and conduct interviews.

Preserve the evidence and protect the privilege (if need be).

- Send a document preservation notice to people who may have relevant information if you think there's a threat of litigation. However, keep in mind that such notices can often generate office speculation or gossip and should be thoughtfully drafted.
- Work quickly and closely with your IT, HR, and Records departments to suspend any regular data disposition procedures, ensure information from custodians who are separating from the company is maintained, and collect potentially relevant documents and communications. Engage an electronic discovery provider to perform the collections if you do not have the necessary in-house expertise.
- Consider whether employees' personal mobile devices may contain texts, chats, or other relevant information not otherwise accessible to your IT department, and if so, whether you bring your own device (BYOD) policy requires employees to make those devices available for inspection.
- Decide if the investigation should be conducted under the attorney-client privilege. Not all investigations need to be, but if the stakes are high or litigation is threatened, a privileged investigation may be necessary.
- For privileged investigations, make sure that the privilege sticks. In-house or outside counsel can create the privilege but copying in-house counsel on correspondence will not suffice. The attorney must be actively involved with, and advising on, the investigation for the privilege claim to be clear.
- If the investigation requires outside experts (for example, forensic accountants), it is preferable that such experts be retained by counsel to preserve the privilege. To minimize risk of a privilege waiver, experts must act as agents for counsel and work under counsel's control and direction for the purpose of assisting counsel in providing legal advice.

Gather documents and interview the witnesses.

- Early interviews can be invaluable to lock in recollections and better understand what needs to be investigated. But some interviews are best conducted after a thorough review and analysis of relevant documents. In either event, give thought to how interviews are sequenced.
- Give all corporate witnesses an "Upjohn" warning if the interview is being conducted by an attorney, and make sure that witnesses understand the role of each person in the room.
- Build rapport, ask follow-up questions, and make sure that you understand the witnesses' statements. Remember that no one enjoys being interviewed for an investigation — be thorough and persistent, but also professional and patient.

Make credibility determinations, factual findings, and conclusions.

- Internal investigations do not carry a "beyond a reasonable doubt" burden of proof, but the investigator should reach well-supported, principled, and unbiased conclusions. This is why choosing the right investigator from the start matters.
- Conclusions should be concise and specific and cite to relevant documents and witnesses. Sometimes investigations are inconclusive, and that is acceptable too.

Report the conclusions and advise on next steps.

- Decide whether final reports should be oral or written — there are advantages and disadvantages to each.
- Final reports — whether oral or written — should only be shared with the people who need to make decisions about next steps. Generally, reports should not be widely disseminated and should stay within the company.
- In most cases, it is appropriate to tell the person who raised the complaint and the person(s) who is the target of the complaint that the investigation is closed. Depending on the complaint and the investigation results, you may not want to share the findings.
- If the investigation confirms that there was improper, unethical, or illegal conduct, the company should consider its disclosure obligations (if required by law or otherwise advisable) and appropriate remediation, including (among other things) employee discipline, enhanced compliance controls, or further employee training.

What to Do When the Government Comes Knocking

A Reference Guide for Search Warrants

- **Review the warrant**

  If state or federal law enforcement agents arrive and announce a search of your home, office or business, ask to see a copy of the search warrant and the agents' credentials.

  The warrant will be bare-bones but it must specifically identify the place(s) to be searched, the things to be seized, and the date range within which the search must occur. Never consent to an expansion of the search.

- **Cooperate**

  Disputes regarding the scope of the search must be brought to the attention of the prosecutor or the court to be settled. Do not prevent the agents from searching areas they claim to have the right to search.

  A warrant is the equivalent of a court order from a judge, and you must obey it. Unlike subpoenas, search warrants can be executed immediately by the agents who present the warrant to the party to be searched. Expect several agents to arrive at the place to be searched and take files or records. Agents may even remove entire computer systems without advance warning.

- **Identify a responsible official**

  Identify one company official to interact with the agents. Inform the agents and employees that any questions from law enforcement should be directed to that person. Be sure the office manager or highest-ranking employee on the premises is informed of the situation.

- **Consult counsel**

  Immediately contact experienced counsel on a private phone, out of the agents' earshot.

- **Know your right to remain silent**

  A search warrant cannot compel anyone, including officers or employees, to speak to or be interviewed by the agents. However, providing certain limited information upon request — such as the location or names of key computer files or databases — may minimize the disruption to your business (e.g., enabling the agents to "image" rather than seize your computers).

  Employees are not required to explain the operations of the company, bookkeeping, records, or the meaning of any document. Advise officers and employees that while they have the right to speak to the agents, they cannot be compelled to do so, and they are free to decline any request for an interview. Do not instruct anyone to refrain from speaking to the agents, or you may face criminal liability. It can be a criminal offense to instruct another person not to speak with law enforcement.

- **Avoid obstruction**

  You may observe the agents during the search and take notes of their activities if doing so does not interfere with the search.

  Never remove, discard, or hide any objects or documents that might be subject to the search warrant.

- **Attempt to safeguard privileges**

  If the search involves information subject to the company's attorney-client or work-product privileges, you should notify the agents of such status, and request that they not review, copy, or seize that information. In all instances, carefully document any seizure of privileged material, including the imaging of any electronic devices that might contain privileged material.

- **Request inventory**

  The agents will prepare a cursory inventory of the items they seized. You can and should request a copy of it. When the search is concluded, request a meeting with the lead agent to review the inventory and to ensure its accuracy.

- **Do not sign anything**

  You have no legal obligation to sign any statement in connection with the execution of a search warrant, including the receipt or inventory list of items seized; rather, request a copy of all documents you are asked to sign and provide the copy to your attorney as soon as possible.

- **Preserve records**

  Once the company has knowledge of a criminal investigation, it must take steps to preserve all potentially relevant paper and electronic documents and information, and it must suspend usual records disposal and auto-delete procedures to avoid the appearance of obstruction of justice. Outside experts should be engaged where necessary to ensure that all potentially relevant information is preserved without any inadvertent alteration of metadata.