The Future of Investigations

By Alex Gershner & Bob Sprague

This valuable thought leadership is derived from our Spring 2023 Forensics Institute webinar series. We hope you enjoy this article and hope to see you on a future live Forensics Institute webinar.

At **FORVIS**, we asked ourselves: What does the future of investigations look like to us? We've identified some key areas of change and risk you'll want to be familiar with.

Understanding the Investigation Life Cycle

Before diving into future developments, an introduction to the typical investigation life cycle is helpful. Here is a brief overview of the five stages of the investigative life cycle: *(1) scoping & planning, (2) collecting & preserving data/ evidence, (3) fact finding, (4) reporting, (5) remediation.*

1. **Scoping & Planning**

   There are five key questions investigation teams should consider addressing before or at the onset of an investigation:

   a) What is the objective?

   b) Who are the stakeholders?

   c) Does the investigation team have requisite competence and independence?

   d) Has management been appropriately quarantined from the investigation and who has oversight?

   e) Will there be a root cause analysis of how issues occurred, as compared to simply confirming what occurred?

   Additional considerations include performing a preliminary evaluation of the merit of the known or alleged issues, establishing a hierarchy of priorities and a rough timeline or preliminary order of operations, and addressing the unique nature of internal investigations in response to a government investigation or inquiry.

2. **Collecting & Preserving Data/Evidence**

   While each investigation takes its own course, perhaps the most important element of any investigation is confirming that the potentially responsive and relevant evidence is preserved and collected for use during the fact-finding stage. The data-related steps can be the costliest component of an investigation when considering the collection, processing, and the review of information that is responsive to the investigation issues. When thinking about collecting and preserving data, there are three primary sources of evidence or data that our team is concerned with: conducting interviews, electronically stored information (ESI), and paper or hard copy documents.

   a) Conducting Interviews

      Interviews will likely occur throughout an investigation, but the earlier interviews serve to gather facts and background information at a time when those are not yet established. The early interviews help the investigation team understand who within the organization may have relevant data and where the data is located, including the specific devices or servers. Interviews later in the investigation life cycle will be more focused on addressing issues at the heart of the investigation, solidifying the facts, and potentially seeking confessions from those involved in the alleged wrongdoing.

FORVIS is a trademark of FORVIS, LLP, registered with the U.S. Patent and Trademark Office.

b) ESI

ESI includes any type of electronic data such as email, accounting system data, employee time records, and other business operating data. During this critical time period, it is important that all data that may be relevant to the investigation is preserved. Organizations, through in-house or outside counsel, will often send out a document preservation notice, which alerts and requires those who may have relevant data to preserve that data. Typically, the collection of ESI is accomplished by a company's IT department with oversight from the investigation team, including digital forensics professionals. IT departments also should pause processes around automatic archiving or automatic deletion of data that may ultimately be relevant.

c) Paper Documents

Although most documents can be made available electronically, there are times when certain paper documents must be physically collected or analyzed on site. This is especially important when documents may contain contemporaneous handwritten notes and edits or have physical characteristics that are difficult to assess through an image.

Thorough and complete data collection is key, but over-collecting data can be costly and time-consuming. To help reduce inefficiencies, our team culls data by processing everything that is collected, running search terms, and evaluating a smaller but relevant subset of the information collected. Sophisticated analytics tools that utilize machine-learning techniques can help with identifying information and data that are relevant to the investigation, further limiting the number of documents that need to be manually reviewed.

3. Fact Finding

This phase often includes:

- Reviewing documents and information
- Analyzing the information based on the agreed-upon scope and making potential scope adjustments
- Considering whether you have already received or expect to potentially receive a government subpoena, including developing the response plan

During most investigations, there will be additional rounds of data and evidence collection based on analysis of earlier information received. Additional interviews are conducted during this phase. The investigation team will decide on the appropriate timing and order of interviews and typically prefers the "funnel approach" to the order of the interviews and the interview question line. That begins with individuals on the periphery of the issues and progresses toward individuals with expected tangible knowledge and involvement.

Establishing a communication plan, including the frequency, mode, and audience of communication, is essential. Communications should be factual and on topic, especially written communications. In instances where external communications occur, whether that be to regulators, clients, or other stakeholders, these considerations take on additional significance, including privilege considerations that should be discussed with counsel.

FORVIS is a trademark of FORVIS, LLP, registered with the U.S. Patent and Trademark Office.

4. **Reporting**

   The reporting process typically includes periodic interim reporting to certain stakeholders, but often culminates in a final oral, written, or hybrid reporting to certain stakeholders, *e.g.*, a board, regulators, executives, etc. The content and the type of reporting should be carefully considered. Other considerations may include maintaining privilege, satisfying auditors, and regulatory requirements. We are frequently engaged through attorneys to help maintain privilege over our work.

5. **Remediation**

   Remediation is the final step for most investigations. When possible, once the root cause is established, the organization should begin remediating the identified issues to both mitigate the risk of reoccurrence and to demonstrate to regulators and other third parties that the organization takes the situation seriously. The speed, breadth, and depth of remediation continue to be factors that regulators and other third parties consider when evaluating actions related to the organization.

   In many routine investigations, remediation is limited to fixing deficiencies in the existing internal control environment or implementing new controls. Training, communication, security, and cultural assessments may be required for investigations with more significant issues.

Some additional suggestions and ways to help avoid pitfalls during an investigation include:

- Handle evidence with care
- Remain objective
- Follow the facts
- And don't prejudge the issues

Regulators expect independence and objectivity by the investigation team. Often, regulators will rely on the investigation team to present the facts, but if regulators believe the investigation team has lost objectivity, they will likely take a more active stance in the investigation. Losing objectivity, whether it be actual or solely in appearance, is one of the easiest ways to lose credibility.

Understanding Evolving Risks

The pandemic presented novel challenges and risks and changed the way investigations are performed. As we have emerged from the pandemic, many companies have never returned to a full, in-person work environment.

Through a traditional lens, the hybrid work environment makes it difficult to monitor individuals and identify suspicious behavior when you are not interacting with them in person and, in some cases, literally looking over their shoulders. Working remotely also may make your staff more vulnerable to external bad actors, *e.g.*, phishing and cyberattacks. In addition, traditional internal controls are structured for in-person work environment, *e.g.*, manual paper signoffs on a bank reconciliation.

Through a modern lens, advances in software and technology help improve the ability to virtually monitor individuals. Given the increases to hybrid and remote work arrangements, this monitoring software is more commonplace than just a few years ago. Examples of these tools and technology advances include:

- Screenshots of employee screens occurring at regular intervals or as a result of triggers
- Keystroke monitoring, which can log and monitor all keystrokes, independent of that individual's actual "end product," *e.g.*, the actual email they send or document they finalize
- Data loss prevention (DLP) describes a suite of tools used by organizations to prevent and detect the unintentional or intentional improper sharing, misuse, or improper access to data

FORVIS is a trademark of FORVIS, LLP, registered with the U.S. Patent and Trademark Office.

Single sign-on (SSO) has become more commonplace. In short, this is an authentication method to access multiple applications and sites with one set of credentials. For example, organizations may have Google or Microsoft SSO capabilities. There are several pros and cons to SSOs, but from an investigatory standpoint, the pros outweigh the cons. For example, an IT admin at an organization can cut off an individual's access to many organization applications and sites at once. In addition, a component of SSOs are audit logs that can track user and account action across a particular service. In one interface, an IT admin may be able to view all email, instant message, and browser activity for a particular user. It also is possible to extract this activity for use during an investigation

Logs and software of this nature can be very important. Many companies have them, but often, the individuals who are part of the investigation team may not know they exist. It is imperative to ask questions to understand what features, applications, and logs are stored.

Preparing for Evolving Risks

One thing is for certain—the risks that organizations face are constantly evolving and vigilance is required to address these risks. Below are some considerations for organizations preparing for evolving risks:

Training

Organizations should train their personnel to look out for suspicious communications or behavior. Organizations also should confirm their personnel are empowered to report anything suspicious and without negative repercussions—this should be communicated frequently and clearly.

Establish Internal Committees

No one understands organizations better than their members. Create a cross-functional committee or several different committees to monitor changes that are affecting—or may affect—your organization.

Have a Plan

Consider creating an "Investigations Playbook." While no playbook could outline every aspect of a hypothetical investigation, organizations should consider what may benefit from being documented and prearranged. Your organization also could perform mock internal investigations to confirm it is ready for a real one.

Focus on Compliance Programs

The best compliance program will not prevent all fraud from occurring. However, implementing and maintaining a strong compliance program is important. The U.S. Department of Justice (DOJ) speaks about this frequently, discussing their policies and views to help organizations consider their actions.

As part of its consideration during the penalty phase of investigations, both the DOJ and SEC spend significant time evaluating an organization's corporate compliance program. If an organization can demonstrate that it takes compliance seriously, has strong compliance policies and procedures, and quickly implements remedial measures during and in the aftermath of an investigation, the government will consider this and may provide credit.

If any of these topics are new to an organization, it should consider hiring an outside consultant, like FORVIS, to assist. With a solid history of quality investigatory work, dispute consulting experience, and a variety of technology and tools, our team stands ready to assist. If you have any questions, please reach out to a professional at **forvis.com** today.

FORVIS is a trademark of FORVIS, LLP, registered with the U.S. Patent and Trademark Office.