compliance next™

The Worst-Case Scenario Survival Guide

for Compliance Professionals

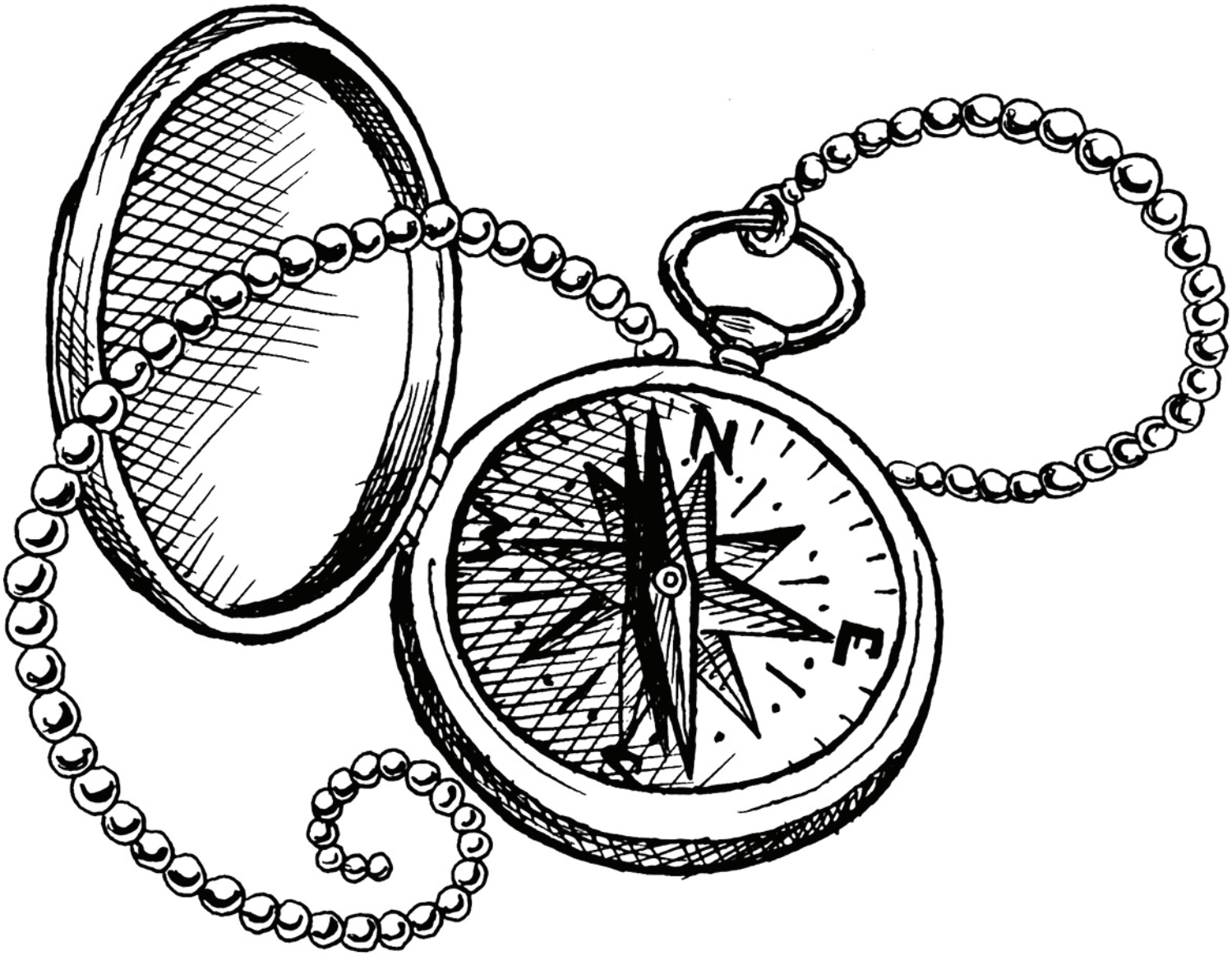

N
E

Table of Contents

Overview

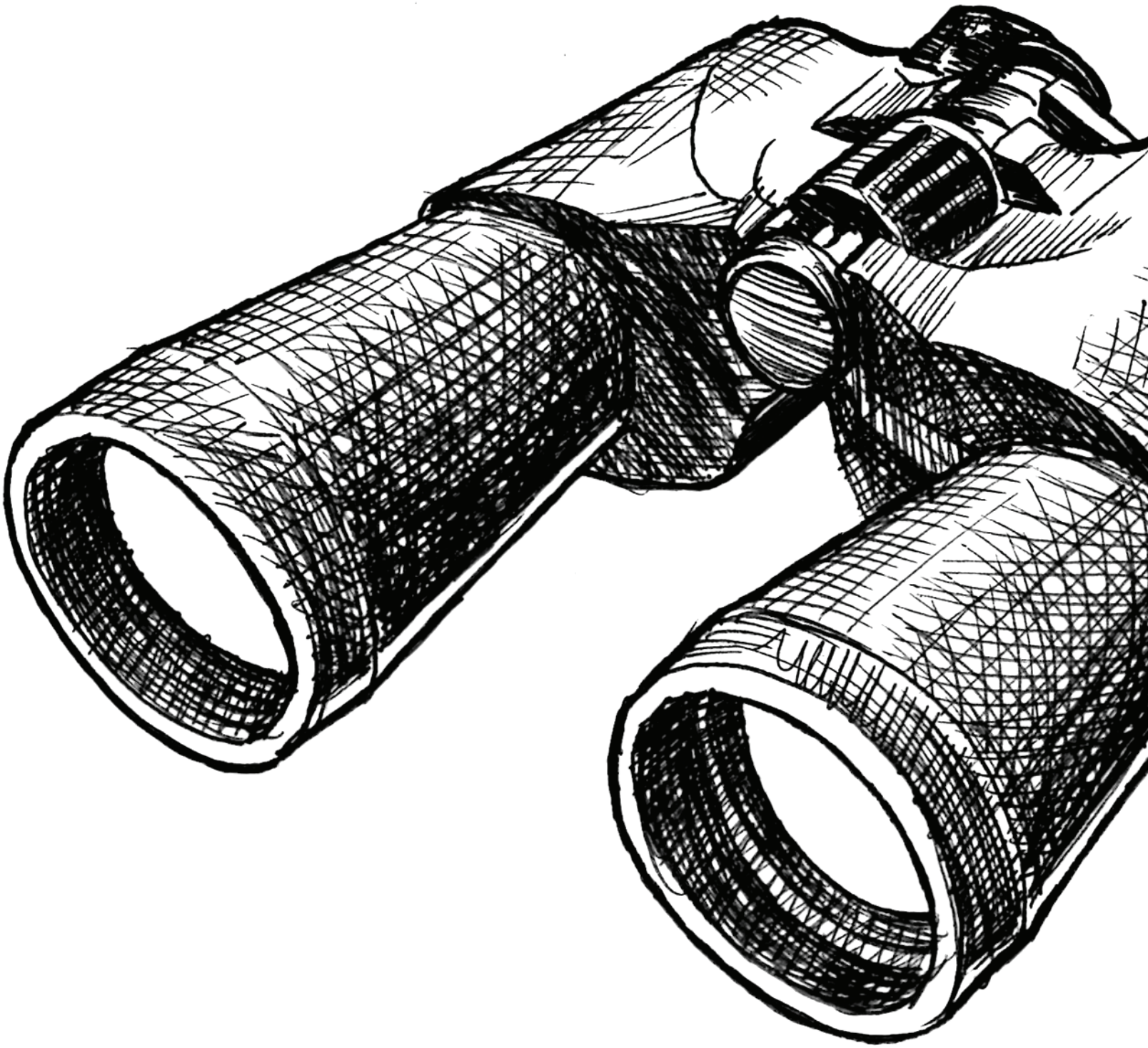
The Worst-Case Scenario Survival Guide for Compliance Professionals is a collection of real-world compliance failures that have been organized into four key compliance program categories: leadership, structure, innovation and integration. Paired with expert commentary from Tom Fox, these pro-tip survival stories reveal what works, and what does not, when it comes to running a top-notch compliance program. Each survival topic found in this guide offers a structured experience to readers where each compliance failure is defined and described, followed by step-by-step best practices on how to survive some of the most complex compliance issues.

Fox combines his real-world compliance perspectives with modern failures across industries to create a unique learning experience for compliance practitioners. Follow these easy to walk through best practice methods for tackling a wide array of compliance variables – before having to experience them yourself. We hope you enjoy this guide and avoid making these all-to-common mistakes.

MEET THE AUTHOR

Thomas Fox, *The Compliance Evangelist*

Thomas Fox has practiced law in Houston for 30 years. He is now an independent consultant, assisting companies with FCPA and compliance issues. He was most recently the general counsel at Drilling Controls Inc., a worldwide oilfield manufacturing and service company. He was involved with compliance investigations, audits, and drafted policies, and he led training on all facets of compliance, including FCPA, export, anti-boycott, and commercial operations training. Fox has the award-winning blogsite, FCPA compliance and ethics blog, and podcast, "The FCPA Compliance and Ethics Report."



Leadership

1 How to Survive a Code of Conduct Violation

You are the Chief Compliance Officer (CCO) of a medium-sized corporation. Sitting in your office on Friday afternoon, you receive a call from the Securities and Exchange Commission (SEC). They want to come by your offices on Monday morning to discuss potential code of conduct violations by your senior management. Further, they tell you that these code of conduct violations may be evidence of ineffective internal controls and therefore a potential FCPA violation. What do you do?

Let's explore how to survive a code of conduct violation and ways to avoid this nerve-wracking situation in the first place.

How to Survive

1. Know Your Code of Conduct

The substance of your code of conduct should be tailored to your company's culture, and both its industry and corporate identity. It should provide a mechanism that encourages employees to do the right thing when it comes to compliance and business ethics. The code of conduct can be used as a basis for employee review and evaluation. Your company's disciplinary procedures must be stated in the code of conduct and should be invoked if there is a violation. Finally, your company's code of conduct should emphasize it will comply with all applicable laws and regulations, wherever it does business.

Your code of conduct should not be written by lawyers for lawyers. It should be tailored to your organization. Most importantly – train on it and use it for all employees.

2. Show Complete Accessibility Throughout the Organization

The SEC has repeatedly noted the most effective codes are clear, concise and accessible to all employees, as well as those conducting business on the company's behalf. This is also true for those with whom you are doing business, so third parties need to be considered when communicating your code of conduct. For those employees who do not speak English, you must translate both the code of conduct and their training into the local language.

Everyone must be able to understand the concepts set out in your code.

3. Provide Detailed Training Records

While many companies understand the need for robust, ongoing training for their compliance program, they do not always have the same rigor around the code of conduct. It may be provided when an employee is on-boarded and then via online training once per year, or even bi-annually. But that alone is not sufficient. And if it is, you should at least have effectiveness metrics to back up your code distribution and training strategy.

Begin with live training that can be held at the corporate headquarters with senior management and executive involvement. Many companies will even videotape a message from the CEO to help celebrate the rollout of a fresh code. Here exists the opportunity for localized training that gives employees an opportunity to see, meet and speak directly with their compliance officer. This type of event turns the training into a more significant dynamic in the

corporate environment. Such personal training also sends a strong message of the organization's commitment to the code of conduct.

4. Display Regular Reviews & Updates

Simply having a code of conduct, together with compliance policies and procedures is not enough. As articulated by former Assistant Attorney General Lanny Breuer, "Your compliance program is a living entity; it should be constantly evolving." The 2012 FCPA Guidance stated, "When assessing a compliance program, the DOJ and SEC will review whether the company Guiding Principles of Enforcement has taken steps to make certain that the code of conduct remains current and effective and whether a company has periodically reviewed and updated its code."

Some of the questions you should consider are: When was the last time your code of conduct was revised? Have there been changes to relevant laws relating to a topic covered in your code of conduct? Are any of the topics covered in your code of conduct outdated?

5. Garner Executive Buy-in for Your Code of Conduct

Breaches in your company's code of conduct can be deemed an FCPA internal controls violation. Entering into FCPA territory brings on enforcement fines, sometimes into the millions of dollars.

This enforcement action makes it clear that if there is an exception made to the code of conduct, it must be approved by the highest level in an organization, the board of directors. Further, if there is a code of conduct violation, there should be appropriate discipline issued.

6. Exhibit an Operationalized Code of Conduct

If you haven't already, work to operationalize your code of conduct, as articulated in the DOJ's Evaluation of Corporate Compliance Programs. The Evaluation focuses not on whether a company has a paper compliance program but on whether a company is actually doing compliance. A company does compliance by moving it into the functional business units as a part of an overall business process. That is what makes a compliance program effective at the business level.

Both the SEC and DOJ expect you to operationalize your code of conduct as you would the rest of your compliance program.

7. The Bottom Line

The cornerstone of every compliance program is the code of conduct. In the 2012 FCPA, the DOJ and SEC said, "A company's code of conduct is often the foundation upon which an effective compliance program is built." More importantly, your code of conduct also serves as an internal control. This means it should be reviewed, trained on and then tested for effectiveness.

The code of conduct is not only a foundational document for your best practice compliance program, but it also acts as an internal control. You need to make sure it is followed closely by consistent training and monitoring. If an exception is taken, it must be appropriately vetted.

Leadership

2 How to Survive a Conflict of Interest

Two new Directors were recently elected to your board and, after introductions, you discover one of the new directors previously ran the local branch of a national bank. He casually mentions a recent personal loan he made to your CEO and board chair before being nominated to the board. From the sound of it, the banker had been falsely advised that the CEO's "new start-up fund" was a company sponsored initiative.

Let's evaluate what you can do immediately to survive.

How to Survive

1. Determine the Conflict

Your conflict of interest policy specifies that there can be no use of company property for personal gain. Further, if any employee engages in an outside business endeavor, it must be approved by an appropriate level corporate committee. For officers, such a conflict must be approved by the board of directors' compliance committee. As the CCO, you have two concerns: (1) is the CEO selling board seats for personal loans and (2) is the CEO's new start-up fund a conflict of interest?

Your conflict of interest applies to everyone, from the boardroom to the shop floor.

2. Define Parameters

You recognize that a conflict of interest may arise from an employee's business or personal relationship with a customer, supplier, competitor, business partner, or other employee, if that relationship impairs the employee's objective business judgment. A conflict of interest may also arise when an employee receives a personal benefit as a result of their position within the company. This includes any loan to, or guarantee of any obligation of, the employee and/or the employee's friend or family member. These problems are only compounded when it involves an officer who is the CEO and board chair.

Conflicts of interest are real and present dangers.

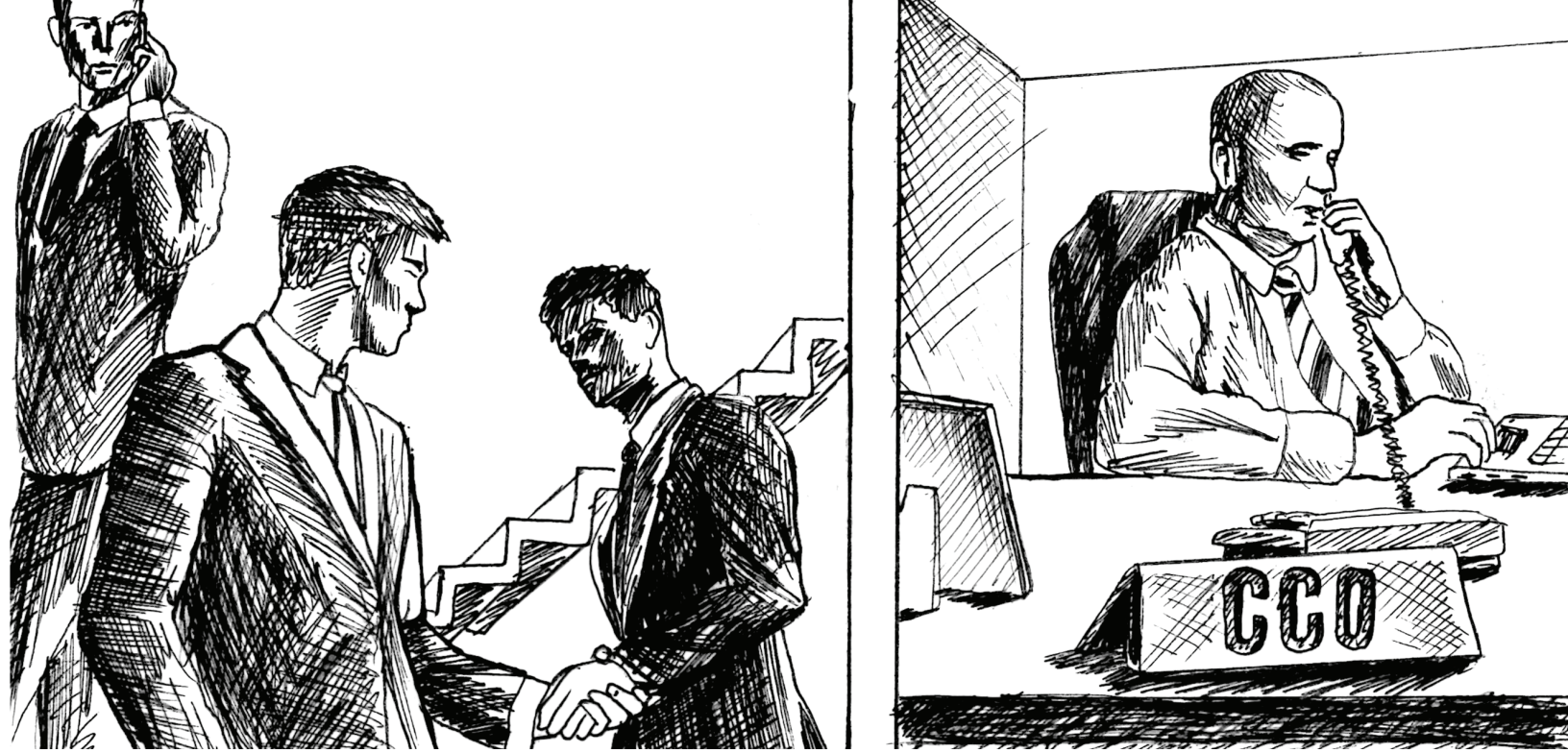
3. Investigate & Review the Situation

Even if you do not believe there is a conflict of interest, as this involves the CEO and board chair, is there a potential conflict of interest? How about the perception of a conflict of interest? Furthermore, what discipline, if any, should you deliver to the CEO? If the CEO violated the conflict of interest policy, should that person receive a warning letter, suspension or termination? If you do not discipline the CEO what will be the effect going forward on the rest of the employees? Will they take the conflict of interest policy seriously or, indeed, any internal company regulation? What would it say about your company's commitment to ethics and compliance? As you are a public company, is this a reportable event?

Andre Agassi was right, "perception is reality." Even if there is no direct conflict of interest, the perception alone is enough to call into question the judgement of the CEO.

4. Consider Questions From Regulators

If the Department of Justice (DOJ) or Securities and Exchange Commission (SEC) came knocking, how would the company respond? What internal controls exist around the company's conflict of interest policy? Does each employee sign a form confirming that they



are not in violation of the company's conflict of interest policy? Is it something more robust? What would a more robust control look like for a company CEO?

With CEO involvement, this may well be a violation of corporate internal controls and thereby subjecting the company to civil penalties.

5. Approach the Board Compliance Committee

The first call you should make is to the chair of the compliance committee. This demonstrates the importance of a CCO having a direct line reporting into the board compliance committee. It also points out the need to have a professional relationship with the compliance committee chair, such that you can pick up the phone and make the report without fear of retaliation.

This situation demonstrates that if there is a potential violation of the conflict of interest policy, it must be reported to the highest level in an organization.

6. Open the Investigation

The chair of the compliance committee should immediately engage outside counsel, who is not doing any other legal work for the company, to conduct an investigation. This investigation must be ring-fenced off so the CEO/board chair does not get wind of it before counsel is ready to interview him. A final report should be made to the entire Board, in executive session, without the CEO/board chair present.

A quick, efficient and thorough review by truly independent outside counsel is mandatory in this situation.

7. The Bottom Line

This is a serious problem for your company. It involves a basic conflict by the top level of your organization. It points to the need for an independent CCO who does not report to the CEO or general counsel but has a direct line reporting to the chairman of the board of director's compliance committee. The violation of the CEO may have been a misstep in judgment, but that type of misstep could be very costly for the company in the eyes of regulators and stakeholders.

The conflict of interest policy is a foundational document for every company. If a CEO violates it, the response must be swift and internally consistent with how employees are treated. If the CEO is given special treatment, it will not only destroy the validity of your conflict of interest policy but may well mortally wound your compliance program.

Leadership

3 How to Survive a Cult Leader

A healthy tone from the top is a cornerstone of strong corporate culture. Typically, the tone trickles down from a team of executives but sometimes the tone emanates from a single individual. This can be dangerous, particularly when that individual is setting the wrong tone.

Let's consider the story of Uber. The scandal shocked us all with reports of harassment, a hostile work environment and violations of basic business standards. People wanted to know, "How is it possible that this behavior was permitted?" To answer that question, we have to take a look at who had the most influence on Uber's culture – former CEO Travis Kalanick.

Kalanick's win-at-all-costs attitude may have contributed to Uber's early success, but it became more of an Achilles heel as the company grew. Like so many visionary leaders who shoot to the top only to fall from grace, Kalanick's influence and tone permeated throughout the company which resulted in an unhealthy work environment – and resounding damage to Uber's reputation.

How to Survive

1. Build and Use Your (Corporate) Backbone

The backbone of every compliance program is its policies and procedures. Coupled with internal controls, these all operate to prevent both illegal and unethical conduct. Policies and procedures make a business run more efficiently and at the end of the day, contributes to a healthy culture. Having such controls in place can allow for fast-growth to move forward in a compliant manner.

In the case of Uber, the organization was built on an improvised approach to management that transcended internal controls. Putting effective policies and procedures in place ensures rules apply to all individuals at every level of the organization, including the leader.

2. Call for Back Up

Sometimes you just need some experienced professionals in the room, like your board. However, the board is not simply there to be a backstop. Board members are seasoned professionals who not only bring business acumen into a situation, but they also provide counsel on the soft skills that can take a business leader from good to great.

The Uber board stepped up and told Kalanick he had to resign as CEO, not simply take an extended leave of absence. The result was reallocating responsibilities to provide a broader, more reliable tone from the top.

3. Avoid Growing Pains

One of the keys to making a startup successful is the ability to scale correctly. Smaller companies need to begin thinking about building a compliance program early on. This means starting off on the right foot with a strong code of conduct, a functional HR department that meets the minimum standard for following U.S. and state employment law, and a CFO to bring financial discipline into the company.

Uber was emblematic of not only of the Silicon Valley "baller" culture (aka frat boy, alpha-male culture), but also of a successful startup that grew faster than its compliance program and ethical culture. Given the proper safeguards, Uber may have been able to avoid

their recent horrors if they had developed a proactive, robust ethics and compliance program before their rapid expansion.

4. Speak Truth to Power

No one, no matter how brilliant or creative, is infallible. Granting Steve Jobs-like deference to a leader is dangerous; all companies need a system of checks and balances for people in power.

The job of a compliance professional is sometimes to take positions that senior executives do not agree with. Yet you must have the courage of your convictions.

In Uber's case, there was no CCO, compliance department or anyone charged with restraining organizational powers from undermining the culture with corrupt and unethical behavior. This kind of gap in leadership led to the development of the very toxic culture driven by Kalanick himself.

5. Go Public

There are many requirements put on a public company which are not required of a private company. Some requirements include comprehensive financial reporting, effective internal controls and many key corporate positions including a CCO. When a company goes public there are a new set of stakeholders involved, the shareholders and their representatives, and a board of directors. Get them involved.

One of the reasons Uber was able to continue for so long in its ways was that it never became a public company. Today, boards and investors may well insist that a company go public to better protect their investments, in addition to being able to make a large pile of cash from the inevitable IPO of a successful startup.

Structure

4 How to Survive the Pitfalls of Gifts, Travel & Entertainment

The FCPA world is littered with enforcement actions against companies for the most basic of compliance failures – those around gifts, travel and entertainment (GTE). Many compliance professionals struggle with issues from GTE: Violations can arise out of anything from discrepancies between outbound and inbound reporting to simply relying too heavily on the manual process of maintaining spreadsheets.

How to Survive

1. Document, Document, Document

You have policies in place – great. Now prove that you follow them. It is not the government's responsibility to prove that you violated the FCPA. It is your responsibility to prove that you didn't. This means you need to document both the existence of your compliance program as well as its effectiveness. For instance, if your company provides travel to foreign officials, you need to document the exact business purpose of that travel or it could become problematic.

2. Don't Go to Disneyland Unless Your Office is in Tomorrowland

There is nothing to prevent your company from bringing foreign government officials to the U.S. or any other facility to attend meetings, observe your manufacturing process or to provide training. The key is that you must actually have facilities in those locations. That mean no trips to Disneyland, Las Vegas, the Grand Canyon or any other location where you do not have physical facilities.[1]

3. Make Sure Expenses are Relative to Where they are Being Spent

You can make some cash payments to foreign officials for travel expenses but they must be small ($50 or less), and you must have documented receipts for the expenditures. Consider the relative value of the cash you provide compared to the annual income of the country from where the officials are traveling. This means that if you give an official $100 and the country's annual per capita income is less than $1,000, you have a problem.[2]

4. Add Up all the Small Things

Many companies are comfortable with small gifts of up to $250, which can be given without pre-approval. However, even small gifts can add up to large overall dollar amounts. How is your company assessing how much is spent by one business unit, department or group in total? Are you tracking how much is spent on one government official, one government department or business unit of a state-owned enterprise? The aggregate amount must be determined and reviewed. In the GTE compliance world, size matters.[3]

5. Trust but Verify

Most companies require employees to report GTE provided to foreign officials or employees of state-owned enterprises. However, are you certain your own employees are reporting correctly and accurately? What if your company decided to reconcile its outbound GTE register (the GTE given) with its inbound GTE register (the amount your internal expense system says you have given)? If there is a discrepancy, you may have a problem.

Employees are always eager to get their money back, but they may be far less eager to complete the necessary records. While some companies have a direct linkage between their expense system and GTE register, many still do not. It is this sort of exposure that companies continue to face, with often significant consequences.

6. Take a Look Behind Your Own Curtain

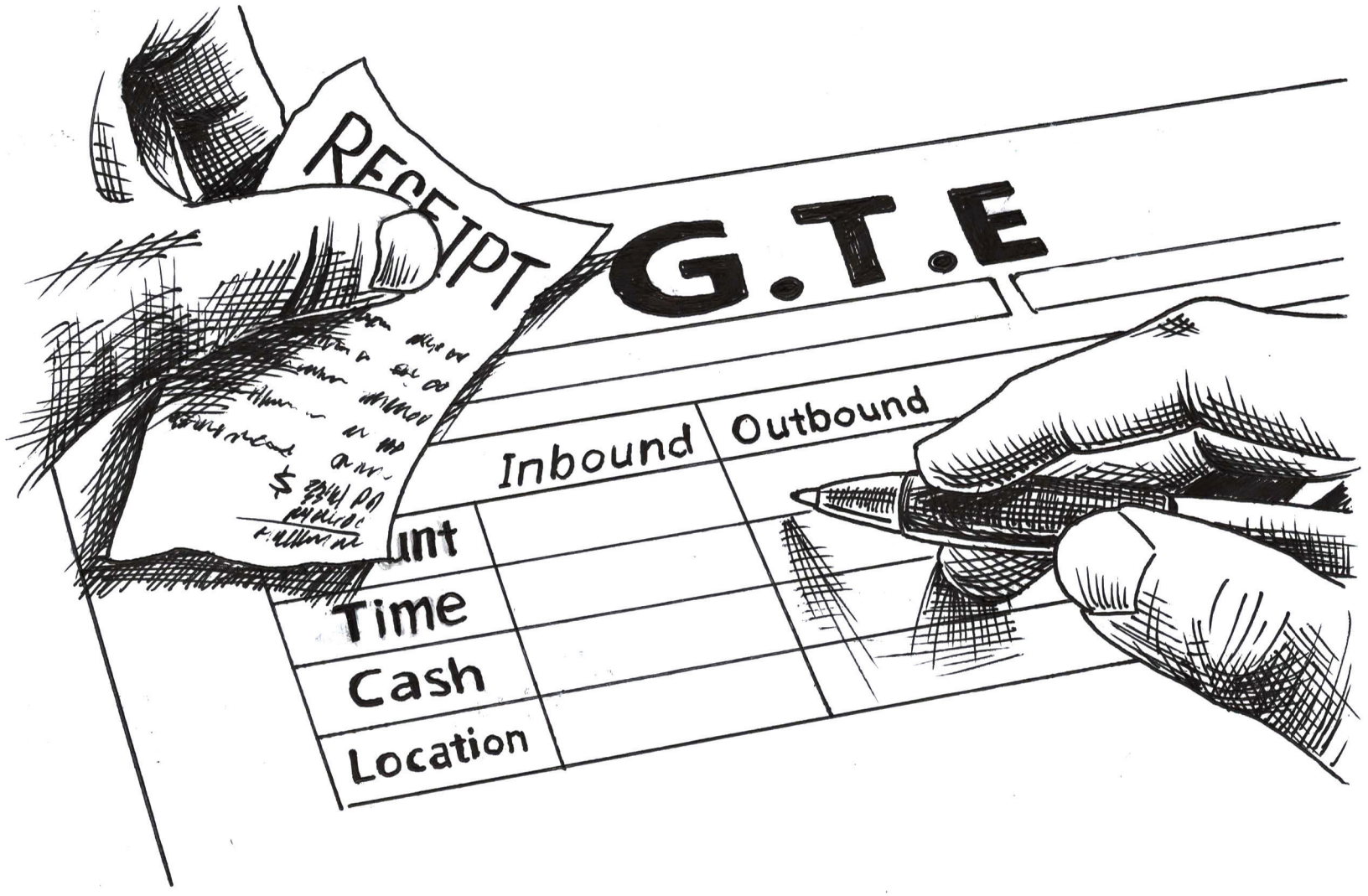
GTE issues not only arise in the FCPA context, but also for U.S. companies under their own internal conflict of interest policies. If there is large GTE provided to your employees from your vendors, there may be a conflict of interest or simply the appearance of impropriety. This is why such GTE must be reported and often times pre-approved before the vendor GTE spending occurs.

Something as simple as your security logs for visitors can provide significant insight into these discrepancies. If there is a log entry notation that a vendor came to your facilities on a certain date at any time between 11 AM to 2 PM to see a certain employee, cross-reference to see if that employee reported a GTE receipt in the form of a lunch or other gratuity. Another method would be to consider the GTE spends on comparable departments. If there is a large discrepancy, this could be a red flag which requires a further investigation.

[1] Based on the Lucent FCPA enforcement action, https://www.sec.gov/litigation/litreleases/2007/lr20414.htm

[2] Based on the ABB FCPA enforcement action, https://www.sec.gov/litigation/complaints/comp18775.pdf

[3] Based on the Diageo FCPA enforcement action, https://www.sec.gov/news/press/2011/2011-158.htm



Structure

5 How to Survive a Rogue Third-Party Agent

You're reading through your morning email when you see this terrible subject line: "Hey, don't we use this sales agent?" That's when you read the details of an email describing a third-party sales agent you know very well who has facilitated an illegal bribe for one of your competitors. Now, both the competitor and the sales agent are the focus of a recent FCPA enforcement action. It's bad news, and it's only a matter of time before your company is affected. What do you do?

How to Survive

1. Dig into the Past

Did you take the right steps when you initially approved this third party? You'll want to backtrack and confirm that your approval process included a written explanation of the business need for the sales agent, as well as a fully answered questionnaire completed and returned from the sales agent. Did you perform an appropriate level of due diligence review based upon the information in the questionnaire? Next, look to see if that due diligence was internally reviewed, did it contain in any red flags, and if so, were they appropriately cleared? Finally, review the compliance terms and conditions, which should include a right-to-audit clause, annual certifications and other Justice Department mandated compliance terms and conditions.

2. Sniff Around

Start by reviewing previous audits to ensure that no prior FCPA violations exist and that annual compliance training had been completed. From there, run an enhanced due diligence search to see if there is anything new since you completed your initial due diligence on the sales agent's history and note any red flags. Then, follow the numbers. See what payments have been made to the third party. Is there anything not justified per the terms of the contract? Were any of the payments made to offshore locations? Has there been any increase in the percentage commission rate since the contract had been executed?

If payment has been made, make sure it was within the contract terms. Confirm that all payments made to the third-party match up to a properly submitted invoice. Check if all the services mandated under the contract, or described in an invoice, actually delivered to or performed on behalf of your organization.

Finally, verify an annual compliance training certification exists along and confirm that no known FCPA violations related to the third party's representation of your company.

3. Look at Sales

A sales spike in a high-risk area can be evidence of bribe payments. Sales numbers may seem to have maintained a steady rate, but that doesn't mean everything is kosher. Cross-check the third party's invoices against GTE spend by your employees in that country. Specifically GTE involving government officials or employees of state-owned enterprises. As an additional check, look to see if there was any unaccounted spike in the marketing or charitable donation budget for the third party.

4. Loop in Your Team

Now that you know of the potential risk to your organization, don't keep it to yourself. Think of it as being put on notice of a potential FCPA violation. Send an email to your internal audit folks and put the third party on the next audit review. Loop in the business representative to make sure they are communicating your expectations on compliance and ethical business practices. Finally go to your internal controls team to see if there are any detect or prevent controls which might warrant tightening up.

The bottom line is if you are using a sales agent who is under a FCPA cloud you will be held to be on notice for any actions they engage in on behalf of your company.

Structure

6 How to Survive Compliance Training Disillusionment

Employees need to feel personally connected to the notion of doing business ethically and in compliance for your program to be effective. But how can we do this if there is cynicism around one of our most powerful tools – training? Or what if your compliance training is so ineffective as to be rendered useless? Using one of the most well-worn techniques since the invention of fire—that of storytelling is a way to expand your training footprint in a way that engages and educates employees.

Storytelling integrates familiar, real-world examples into your compliance training to create a meaningful and relatable experience for learners. Done strategically, this will increase trust in your internal compliance brand, engage learners and actually change behavior. Let's talk about how exactly storytelling can bring your training to life in a best practice compliance training program.

How to Survive

1. Gather Content

Take advantage of your data resources. Find compelling stories in the compliance information already available to you. As an example, consider the perception of your hotline reports. Not all hotline reports are of illegal, unethical or fraudulent conduct. A substantiated report may be based on perceived unfairness or favoritism in the workplace by an employee. By dispelling the assumption that hotlines are only for the most severe infractions, you can cultivate a steady information source straight from your employees while boosting corporate morale. But don't stop there. Use current events, literally from the front page of today's newspapers to craft compelling compliance stories.

2. Present the Story

Get creative with how you use storytelling in your training. A great example is when the VW emissions scandal came to light. In Houston, CenterPoint Energy, a company completely unrelated to the auto manufacturing business, used the ethical failures at VW as an impetus to release a 2015 video proactively addressing their upstanding culture and values as an organization. They turned the scandal into an opportunity to create awareness of the importance of integrity in their workplace. Along with the published video, CenterPoint Energy also created a resource for management entitled "Manager's Toolkit – What Does Integrity Mean to You?" Managers used this to continually open discussions and foster ongoing conversations focused on workplace integrity.

3. Socialize Your Work

Take the time to share your compliance stories. Try co-authoring shareable content with your employees and showcase how your compliance program drives ethical business practices and fosters an inclusive workplace culture. Tell your compliance program's story and provide your audience with real-world best practice examples they can mimic, through the real-world workday experiences of your employees. Take pride in the work you do and brand your organization as a leader in ethical business practices, through its best ambassadors, your employees. To further enhance this perception both inside and outside your organization, place volunteered examples on your company branded website for maximum impact.

Finally, employees want to hear stories from, and about, their co-workers who've faced compliance challenges and #DoTheRightThing – the hashtag used internally at the award-winning Dun & Bradstreet compliance program.

4. Vocalize Senior Management

Ranging from short messages from your CEO, to videos of your CCO, try using a variety of internal company talent to communicate the concepts of your compliance training program. When a member of senior management shares a message, employees listen. They want to hear the president share a message of commitment to the company's culture and discuss the values behind doing business ethically and in compliance. This is always a message that will resonate with employees. Have your senior management celebrate ethical "wins" for the company by recognizing employees who have done the right thing in a difficult or challenging circumstance.

5. Broadcast Your Secret Sauce

Explore the overlap between your own story-based compliance content and your professional social media strategies. There's an opportunity here for highly effective external communications and internal training. Take the traditional methods of compliance training and combine them with videos and other social media channels to drive awareness with real world examples. If you have an internal twitter function, an internal social media coms system or anything else which is the social media equivalent of an employee bulletin board, post ethics and compliance topics on it. By using real content, it will show your employees not only how compliance standards help them do business ethically, but also how it makes your organization more efficient and profitable.

Remember that people still talk about Homer and Troy because it came down as a story. If you can tell a story around your compliance program, it will resonate more fully with your internal customer base—your employees.

Innovation

7 How to Survive General Data Protection Regulation

You receive an email from your European operations asking if you, as the CCO, are also the company's Data Privacy Officer under GDPR. You look up this acronym and learn it stands for General Data Protection Regulation and that it will go live on May 25, 2018.

While your company has a data protection and data privacy policy applicable under relevant U.S. law, the more you look into GDPR, the more requirements you see in the regulation which are not covered or even addressed in your corporate data protection and privacy policy. What do you do now?

How to Survive

1. Get to Know Your Regulator

Under the new rules, national independent regulators will remain in place. GDPR does not create a centralized EU regulator. A key component of GDPR, however, is that a company only has to deal with one data protection regulator, which is called a "Supervisory Authority" under the new rules. This Supervisory Authority will act as the lead in situations where data-processing crosses the border of EU Member States.

Companies will have to deal with one supervisor, but this supervisor may well be interfacing with other EU watchdogs. This approach is a welcome step forward in terms of simplifying compliance and ensuring consistent application of the new rules by regulators.

2. Get a Handle on the Data You Process & Control

Companies that are data controllers and data processors in the EU, or with EU data, will have more accountabilities and requirements under GDPR. Data processors and controllers must now maintain records of processing activities, according to detailed criteria set out under the new rules, which must also be made available to the Supervisory Authority upon request. Companies that are data controllers must implement technical and administrative measures to demonstrate that the processing of personal data is performed in compliance with the new rules, including the implementation of data protection policies.

As every compliance professional is aware, the three most important parts of any compliance program are the following: Document, Document, Document. This is equally true for GDPR compliance as the documentation of data processing activities, due diligence on suppliers and data processing provisions in contracts will have to be demonstrated.

3. Create New GDPR Specific Policies & Procedures

Companies that control data must implement more rigorous privacy measures for data processing. A new key requirement (and just a great word) is the requirement for "pseudonymization." This refers to the processing of personal data in a way that the data can no longer be attributed to a specific individual without the use of additional information. Further, data controllers will have to implement appropriate measures to ensure only necessary personal data is processed for each specific purpose. Such requirements would include the amount of personal data collected, the extent of processing, the period of storage, and its availability. A company is now also required to ensure that personal data is not made available without that person's approval.

Simply having a U.S. compliant data protection and privacy policy is no longer sufficient, as all of these rights created under GDPR will require the implementation of new internal policies and procedures.

4. Understand the Rights Created under GDPR

There are several new rights you will now need policies and procedures for:

- **Right to Be Forgotten:** An individual or entity can assert the right to have personal data erased without undue delay.

- **Right to Portability:** An individual's right to receive the personal data concerning themselves in a structured, commonly used and machine-readable format. This includes the right to transmit those data to another controller without hindrance from the original data collector.

- **Right to Object:** An individual can object to being profiled, as in the case when personal data is processed for direct marketing purposes.

- **Subject Access Requests (SARs):** A process whereby someone can exercise their right to gain access to data held on them, which must be answered within one month of receipt of the request.

GDPR creates rights which in many ways are antithetical to the manner in which the U.S. engages in business and treats its employees. A major change may be required.

5. Appoint a Data Protection Officer

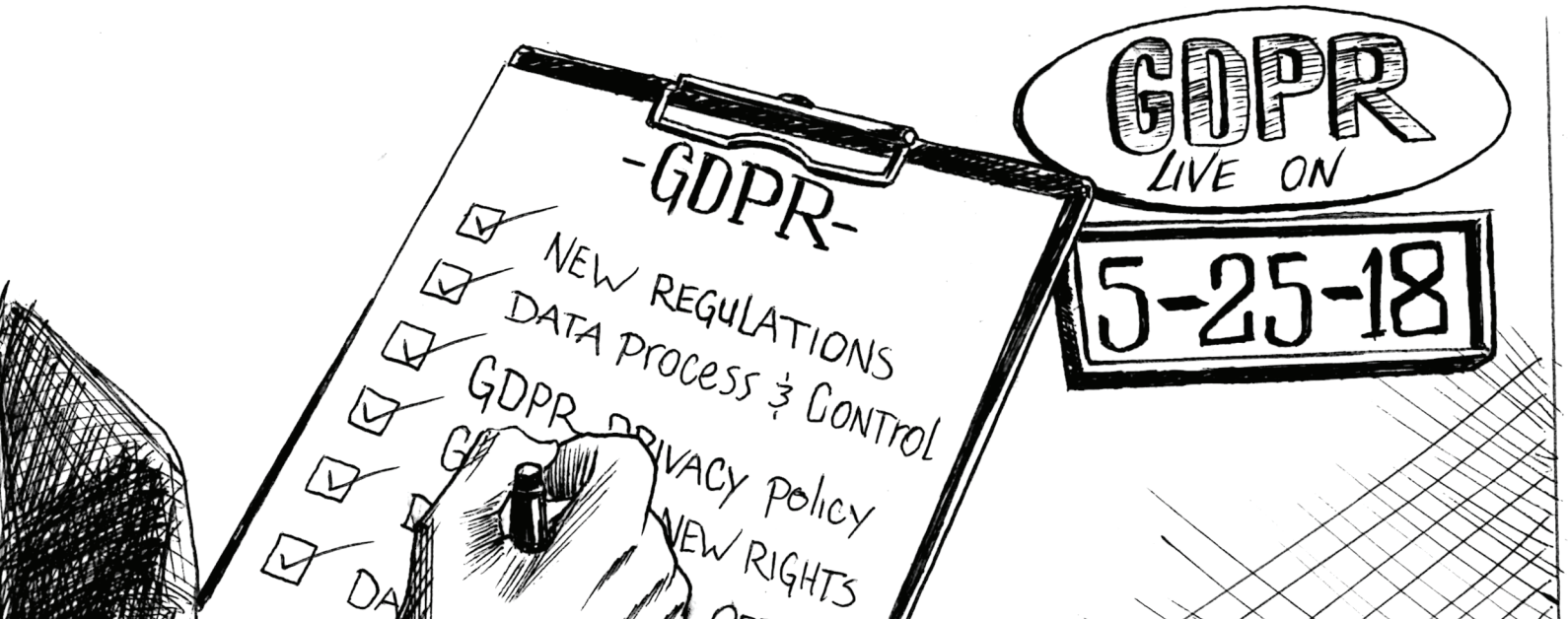
A Data Protection Officer (DPO) should be appointed to deal with data protection compliance. The DPO duties should include oversight and monitoring of the company's data protection and privacy regimes. The DPO must be appropriately qualified and is charged with a number of tasks, including advising on data-processing, data privacy and protection. The DPO must be independent in the performance of their tasks and must also report directly to the highest level of management.

The Data Privacy Officer will be a key corporate position going forward.

6. Report Breaches Within 72 Hours

U.S. companies are notorious for not wanting to report data breaches for fear of reputational fallout. Yahoo!, Equifax, Facebook and Target are all examples of companies that waited months, if not years, to report data breaches. Under GDPR, companies now most report data breaches to an appropriate regulator within 72 hours of becoming aware. This means you will need to put in place a triage team which can quickly and efficiently assess what has happened, so you can meet the requirements of the law.

This reporting requirement will put significant pressure on U.S. companies that sustain such a breach to react quickly with as much information as they can muster at the time. You must put in place a clear data breach action-plan and policy as a top priority and train staff accordingly.



Innovation

8 How to Survive a Root Cause Analysis

In November, 2017, the Justice Department released its new FCPA Corporate Enforcement Policy. Many compliance practitioners have focused on the requirements for obtaining a declination and the discounts in fines and penalties for companies that do not receive a full declination. However, there was other important information every compliance practitioner should pay attention to.

A new area was introduced into compliance programs with the Justice Department's 2017 Evaluation of Corporate Compliance Programs. For the first time, companies that sustain an FCPA violation are required to perform a root cause analysis and incorporate that information back into the compliance program.

How to Survive

1. Know What a Root-Cause Analysis Is

A root cause analysis is a reactive approach to problems. Its purpose is to use problem solving methods to identify the root cause of issues or events. It is based on the belief that problems are best solved by attempting to correct or eliminate root causes, as opposed to merely addressing the more obvious symptoms.

2. Understand the Difference Between a Root Cause Analysis & an Investigation

In an investigation, the goal is to either prove or disprove an allegation. A root cause analysis should not be structured like an investigation, nor should it follow investigative protocols. In an investigation, you are simply gathering facts, not assessing blame. A root cause analysis takes a step beyond gathering the facts to determine how the compliance failure occurred, or was allowed to occur.

3. Find an Approach that Works for You

Keep in mind – there is no one right or wrong away to perform a root cause analysis. However, there are several known strategies such as the "Five-Whys Approach", the "Causal Factors Approach" and the "Ishikawa Diagram." Whichever approach you choose, ensure you apply rigor and do not take shortcuts. Dig, dig and then dig again until you cannot dig any further. At that point, you have determined the root cause and can confidently move onto defining remediation. Do not engage in the "blame game" of simply defaulting to human error. Dig into your polices, procedures and controls to see what led to the compliance failure or allowed it to manifest.

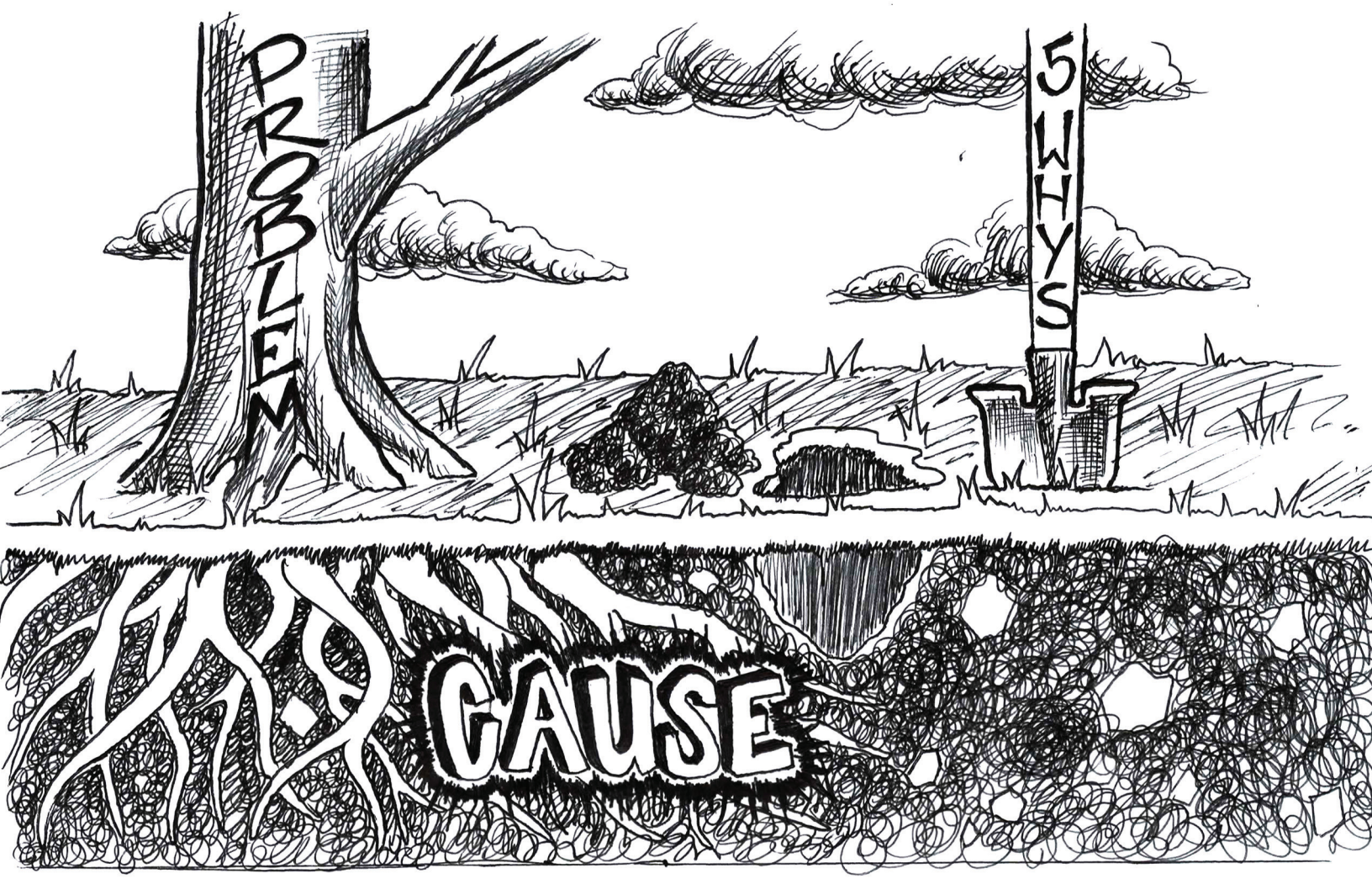
4. Improve Controls, Don't Just Blame People

Don't jump to blaming people for bad systems and processes - unless you uncover willful negligence or gross incompetence. Toughen up, admit that it might be your program, remediate it and move forward. Your employees are doing the actual thinking and processing to generate profits for your company. You do not have to stop their activities nor do you have to penalize with discipline. That is part of the reason a root cause analysis can be such a powerful tool. It identifies what led to the failure without any guesswork.

5. Use the Findings

After you have identified the root cause of a problem, it's key to consider the solutions that can be implemented by logically using data that already exists in the organization. Identify current and future needs for organizational improvement. Your solution should be a repeatable, step-by-step process in which one process can confirm the results of another. Focusing on the corrective measures of root causes is more effective than simply treating the symptoms. You will have a much more robust solution in place. This is because these types of solutions are accomplished through a systematic process with conclusions backed up by evidence.

Under the Evaluation, Prong 1, it stated: **Remediation** – *What specific changes has the company made to reduce the risk that the same or similar issues will not occur in the future? What specific remediation has addressed the issues identified in the root cause and missed opportunity analysis?* The Justice Department clearly expects you to not only perform a root cause analysis for every compliance failure but, more importantly, to also use that information going forward. By following these steps you will survive the root cause analysis requirement of the Evaluation and thrive as an organization.



Innovation

9 How to Survive a Friday Afternoon Cyber Threat

*Let's recall a story that took place a time long, long ago – 2016 – and in places of which few have heard – the U.S., Bangladesh and the Philippines. The story tells the tale of $101 million of Bangladeshi money that was wired out the Federal Reserve Bank of New York (aka the Fed) through the Philippines central bank**. Given the various time zones and locations in play, this fraud took place during the work week and the weekend, which made it even more effective.*

How to Survive

Seventy-five percent of cyber crime is reported as fraud on Friday afternoons.* Let's let that sink in a bit – a single day of the week – a favorite for many – is host to three-quarters of cyber crime reports. Who would have thought? No one … except for wrongdoers.

1. Consider What Day It Is

Is it Friday afternoon? And you're getting an unusual request? This is the first warning sign that danger may be near. Cyber attacks often happen on Friday afternoons because no one's watching the shop on the weekends. If someone is sending you an urgent request late in the week, put up your antennas and perform some additional due diligence for verification.

For example, in Bangladesh the weekend is Friday and Saturday. At the time of the cyber attack, "the computer terminal that connected Bangladesh's central-bank computers to the secure interbank messaging system was 'unresponsive' the morning after the theft" and wasn't able to stop the money transfer.

2. Determine Where the Money Is Going

Were you asked to send funds to a location not specified on the contract, such as a location other than where the services were delivered or where the payee is domiciled? This should raise a red flag.

Of the $101 million, "$20 million [went] to Sri Lanka … to the account of a newly formed nongovernmental organization, according to the officials in Dhaka. The Sri Lankan bank handling the account reported the unusual transaction to the country's central bank and authorities reversed the transfer." Unfortunately the remaining $81 million was wired to a bank in the Philippines.

3. Get to Know Your Vendors and Their Customers

In the banking world "Know Your Customer" (KYC) is a ubiquitous phrase. Yet in the non-banking commercial corporate world, how well do businesses know their third-party vendors, their agents and their customers? As criminals and terrorists become more sophisticated, they are laundering money through commercial organizations and many of these same organizations do not have the internal controls that banks have around anti-money laundering (AML).

The Fed made 35 separate attempts to confirm that the money transfer was legitimate. The Bangladesh Central Bank reconfirm the initial requests to transfer the money before taking off for the weekend. It was not until the work week began on Sunday that Bangladesh Central Bank employees hooked up a backup server and printed out the 35 messages from the Fed. They were able to stop the fraudulent transfers at that point – totally another $950 million -- but $101 million was already gone.

4. Determine if Anything Smells Fishy

There are a lot of physical, digital and human resources that go into processing a money transfer. With all these touchpoints, fraud can tuck itself neatly into nooks we would have never suspected to be tampered with.

According to a report reviewed by The Wall Street Journal, the morning after the theft, "… the senior official in charge of the server room … was concerned when a printer connected to the terminal couldn't print out the interbank messages received during the night."

5. Be Prepared

As with every compliance program, the key to success starts with assessing the risks of your organization. Many compliance practitioners understand this from the anti-corruption compliance perspective. Yet have you considered your risks from the AML perspective? Do you even have a corporate AML policy in place? Have you trained the appropriate employees on it? Do those employees know which countries have Thursday and Friday as their weekend so that if a request for payment comes in late Wednesday afternoon a confirmation may not be available until the next Monday? All of these issues must be considered.

6. Become Your Own Worst Enemy

We usually do not know what's wrong with our processes until someone points them out. Make sure you are that someone, rather than a nefarious actor. Test for weaknesses in your risk management process intensively and regularly so that you are confident in your system at all times of every day of the week.

* Solicitors Regulation Authority (2016). IT Security: Keeping Information and Money Safe

** Wall Street Journal (2016). From the Fed to the Philippines: Bangladesh's Stolen-Money Trail.

Integration

10 How to Survive Internal Reporting System Scrutiny

Your internal reporting system is a key mechanism to fully operationalize your compliance program and meet regulatory requirements. It is essential for obtaining information from employees about potential issues before they become full-blown culture issues or legal violations. An effective reporting mechanism also goes a long way toward engendering trust in your compliance program. This trust is what helps protect a company by motivating employees to use internal channels to report misconduct instead of approaching regulators such as the SEC. Does your current internal reporting system pass the scrutiny of both regulators and employees? Let's review some of the key requirements for a robust internal whistleblower hotline and incident management system.

How to Survive

1. Know the Bottom-line

The clearest statement on the requirement for an internal reporting mechanism is found in the 2012 FCPA Guidance, released jointly by the Justice Department and SEC. It stated, "An effective compliance program should include a mechanism for an organization's employees and others to report suspected or actual misconduct or violations of the company's policies on a confidential basis and without fear of retaliation." But it's much more than simply meeting this legal requirement. A proactive reporting mechanism can help protect the company, as employees will use it to report issues.

An effective internal reporting system is a key best practice that benefits the credibility of your compliance program.

2. Honor Anonymity

Internal reporting must be truly anonymous for those who wish to remain unknown. You can still contact and speak directly with any whistleblower, but you must respect their confidentiality and not attempt to identify them. Attempts to determine the names of whistleblowers will be met with regulatory sanction and weaken your credibility as a compliance function

Do not, I repeat, do not, allow your CEO or anyone else to investigate the identities of anonymous whistleblowers.

3. Publicize Your Hotline

Take concrete steps to publicize your hotline. These steps require documentation so you can show the regulators first-hand when they come knocking. Moreover, clearly delineate the results of your publicity campaign. Are you getting hotline reports, anonymous reports or no reports at all? If issues are not being reported, this could be a key indicator that you need to publicize your internal reporting mechanism more aggressively. Make sure all the phone numbers work and that a mechanism exists for employees who may not have access to a phone or computer.

Get the word out and make absolutely sure the phone numbers work.

4. Ensure No Retaliation

Allowing retaliation against an internal reporter will obliterate the effectiveness of your hotline, and perhaps degrade all trust in your corporate compliance program. Even if the information reported

is not found to violate an internal policy or law, work to ensure there is no retaliation against reporters. This will require the compliance function to work with HR and monitor how the employee is treated for some amount of time going forward. If there is retaliation, you must make it clear that such actions will not be tolerated and that any employee who engages in retaliation will be disciplined.

Work with your HR function and track whistleblower work history to make sure there is no retaliation.

5. Provide Timely Follow-up

Nothing is more frustrating for a whistleblower (anonymous or other) than to never hear back about the information they reported. Acknowledge reports the same day that you get them. After review, if it is deemed worthy of follow-up, contact the reporter and see if they can provide any additional information. If the matter can be investigated and resolved quickly, communicate that expectation with the whistleblower. If it will take longer, communicate that information as well. When the matter is closed, meet with the whistleblower and communicate the final decision – to the extent you can do so.

Make sure you keep whistleblowers informed on a timely basis, otherwise they are more likely to go external.

6. Use Triage & Investigation Protocols

Immediately triage any compliant or information coming through your internal reporting mechanism. Use something as straightforward as low, medium and high risk formulation – or something more sophisticated if preferred. Your triage protocol should get the issue to the right person or group to handle the investigation. The vast majority of your investigations should be concluded in one or two weeks. To accomplish this, have an investigation protocol in place and follow it. If an exception is made, provide a justification for it.

The right information, at the right place, at the right time is critical. Use a robust triage process.

7. Have an Escalation Process

For very serious matters reported internally (and it does happen), an escalation protocol should be in place. Get the report to those who can direct the investigation and be sure to protect the privilege. Even in situations of high significance, you should endeavor to keep the whistleblower informed and protected.

Create and implement your investigation protocol before an investigation is needed.

Integration

11 How to Survive an International Joint Venture

FCPA enforcement actions are littered with companies that came to grief through an international joint venture. The problem starts with the unique structure of a joint venture, which requires the integration of disparate company cultures. This is compounded when your proposed partner is a foreign government of a state-owned enterprise. A joint venture creates a new set of compliance risks for the company that are subject to the FCPA as the company has, by definition, less control. As a result, these issues need to be addressed during the formation of the joint venture. If the company entering the joint venture has less than 50 percent control, issues become even more complex. Let's take a look at five steps you can take to survive an international joint venture.

How to Survive

1. What's Your Justification

Why are you going into business with a foreign partner? In other words, what is your business justification for giving up some of your control and profits? The justification must pass business muster before it goes to the compliance function for compliance scrutiny. Both parties should assess the other and conclusively decide that the joint venture is mutually beneficial and a good fit. This means each side will benefit.

So, how can a company fully protect itself and insure the joint venture will accomplish the business goals? By organizing your approach to a joint venture in a way that mirrors the business reasons for doing so.

2. Perform Due Diligence

The due diligence process should be built on principles like those involving third parties. The procedure should be robust, well-documented and address all potential risks involved. A company should use its due diligence review of the joint venture partner to properly assess and uncover any corruption risk. The risk in joint ventures is primarily that your foreign partner will be a foreign official or employee of a state-owned enterprise. The joint venture will be viewed by U.S. regulators as a mechanism to funnel illegal bribe payments to such a person. You need to take a deep dive into who is becoming your partner, all the way to the ultimate beneficial owner.

3. Terms and Conditions

The joint venture agreement between both parties should have explicit terms and conditions. You'll want these in place for a variety of reasons including the following: (1) to set clear expectations between the parties; (2) to demonstrate the seriousness of the issue to the non-U.S. party; and (3) to provide a financial incentive to do business in a compliant manner.

Consider including these five clauses:

- Absolute prohibition on bribery and corruption
- Full audit rights
- Right to cancel the joint venture agreement if there is material breach and recoupment rights for any FCPA violation
- Clear governance rights if you are a minority partner

- Ongoing, at least annually of certifications from your foreign partner they are not aware of any bribery and corruption

4. Exercise Your Audit Rights

A key tool in successfully managing an international joint venture is auditing. Audit rights are a key clause in any compliance terms and conditions and must be secured. Your compliance audit should be a systematic, independent and documented process for obtaining evidence and evaluating it objectively to determine the extent to which your compliance terms and conditions are followed. You should work to obtain and review the relevant data; analyze and evaluate the data; and use the data as a basis to remediate any issues that have popped up through the operation of the joint venture.

5. Invest in Process

In addition to monitoring and oversight of your joint ventures, you should periodically review the health of your joint venture management program. The robustness of your joint venture management program will go a long way towards preventing, detecting and remediating any compliance issue before it becomes a full-blown FCPA violation. As with all the previous steps, you need to fully document all steps you have taken so that any regulator can review and test your metrics. The Evaluation of Corporate Compliance programs lays out what the U.S. Department of Justine (DOJ) will be reviewing and evaluating going forward for your compliance program. You should also use these metrics to conduct a self-assessment on the state of your compliance program for your joint ventures.

The bottom line is joint ventures present a unique set of FCPA risks for the compliance practitioner. You will need to incorporate risk management techniques in all phases of the joint venture relations; pre-formation, the joint venture agreement and in operations after the joint ventures has begun operation. The compliance obligations and compliance process are ongoing.

Integration

12 How to Survive a 500-Year Compliance Emergency

Are you prepared for the 500-year compliance emergency; i.e., one which has a one in 500 chance of occurring? How about the 1000-year compliance emergency, with the even longer odds of one in a 1000 chance? Over the past three years, the state of Texas has sustained two storms, which are supposed to occur once every 500 years, and one 1000-year storm, which is supposed to occur with even less frequency. What were the chances of these events happening? What are the chances of similar events occurring going forward – like next year? From the compliance perspective if you are doing business in a high-risk country it could be quite high – about as high as Texas having three such storms in three straight years. From the compliance perspective, are you ready for the true emergency?

How to Survive

1. Get Procedures in Writing

You must have a written emergency protocol in place. After all, you're preparing for a true emergency that will easily require more than what a simple investigation protocol can provide. It must include a notification list and a secure communication channel to exchange information across the globe. You need a written protocol so you are not making decisions on the fly during a highly stressful situation. A written protocol will also be important when you're required to demonstrate to the Justice Department that you had a best practice compliance program in place when the incident occurred. This is just the starting point.

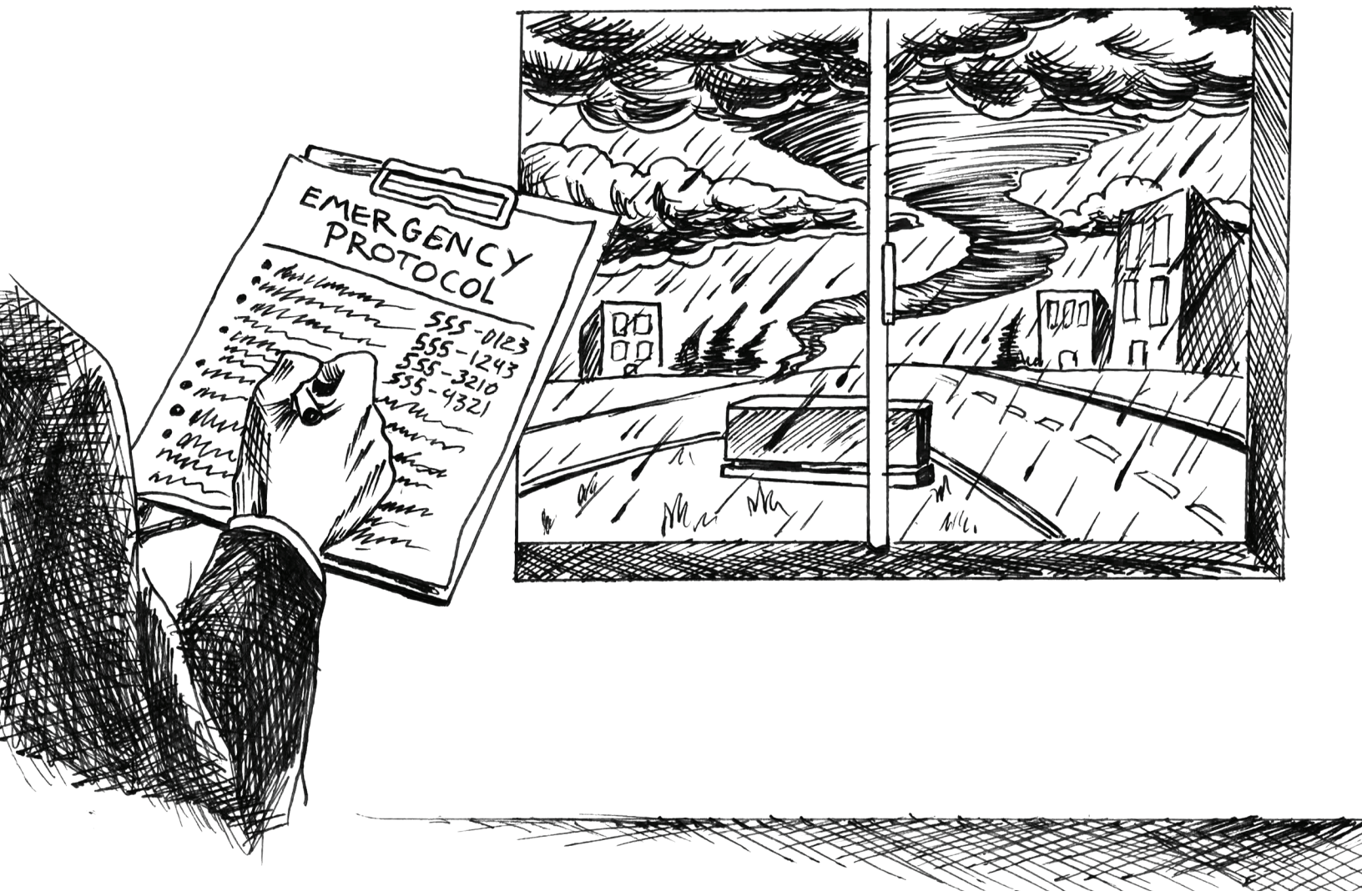
2. Dust that Protocol Off

Take that emergency protocol off the shelf and ask yourself some key questions. Have any of the key compliance risks changed over the past year? Are you in a new geographic area? Do you have a new service being offered to foreign governments? Next, go through your investigation and notification protocols.

When was the last time you updated your contact list for the compliance department – both primary and secondary? How about for senior management, IT, HR, the compliance or audit committee and the full board of directors? What about your key third-party sales agents and suppliers? Now do the same for your primary outside counsel investigative firm and make sure they are ready to respond.

3. Test Your Hotline

Your organization's basic mechanism for obtaining information is through your hotline. However, does it work? How about across the globe? Test it out by making an emergency call from oversees of a major compliance violation. Start with the basics, does your hotline work in every country where you do business? Do you have persons who can speak the language of the caller – either through your hotline service provider or internal to your organization? Finally, does your compliance team receive accurate reports of hotline reported incidents? How quickly does the escalation kick in so that the information gets to you in a timely manner?



4. Secure the Evidence

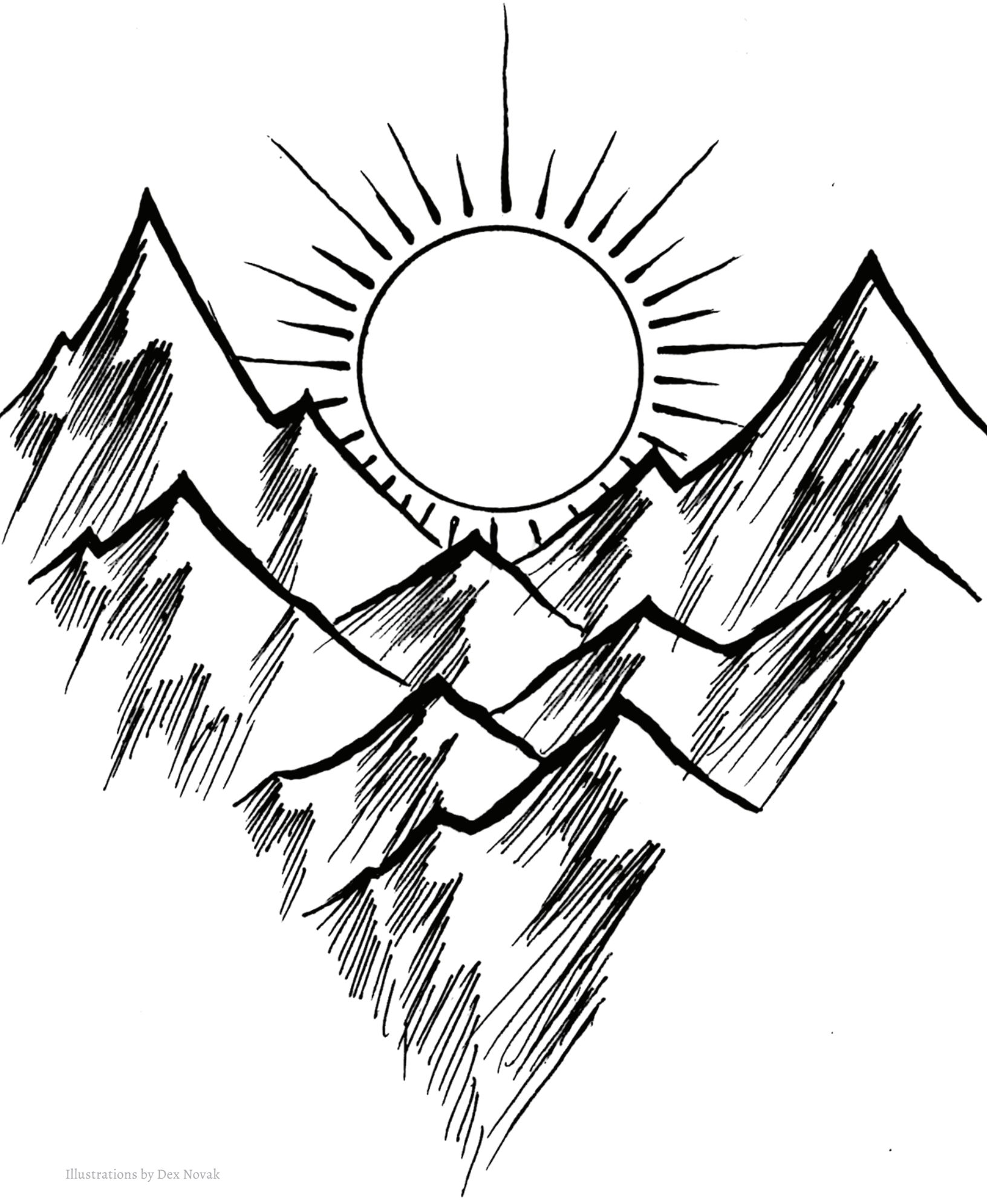
One of the most critical steps going forward will be securing the evidence. This means computer files and written documents. Call your IT folks and get them to freeze everything, even if this is done without the knowledge of the persons impacted or even if their computers are not physically secured. It may be tricky, but you must do so. If you self-disclose, one of the most critical initial conversations with prosecutors will be to convince them you have a handle on evidence security.

5. Practice, Practice, Practice

One of the most powerful lessons learned by FEMA in weather emergencies was that it's not the companies which had written protocols in place that survived, but rather companies that had practiced their emergency responses.

Practice your response by sending a message through your hotline and see how it is tracked all the way up your organization, including up to the compliance committee on the board. Now go through the same exercise with your outside investigative counsel. They should have a preliminary investigation protocol in place which can be adjusted based upon facts on the ground, or at least as they are initially presented.

Finally, make sure your entire team is working off the same playbook. All your response teams, both inside and outside your organization should train and practice together. Don't forget to take advantage of the pronouncement in the Justice Department's Evaluation of Corporate Compliance Program and perform a root cause analysis on the training. If there are any gaps, they should be identified and remediated.



Illustrations by Dex Novak

About This Resource

From regulators and enforcement actions, to cult leaders, rogue third parties, cyber-attacks and conflicts of interest - compliance professionals should always be prepared for the worst-case scenario. These real-world compliance failures can surface at any organization, so we created this e-book to showcase how to effectively navigate a variety of risks using proven, best-practice methods. It is always better to be prepared than to be surprised when danger calls.

Additional Resources: Definitive Guide Series

- **Ethics and Compliance Training: Getting Measurable Value**
  A strong training program is the foundation of an open, ethical and productive culture. Learn how proper training can prevent misconduct, improve employee engagement, strengthen alignment around a set of core values, mitigate risk and promote adherence to compliance objectives.

  Download the Guide to Compliance Training

- **Third-Party Risk Management: How to Successfully Mitigate Risk**
  Help your organization make smart choices when it comes to engaging with business partners. Here, you will learn how to protect your organization from the risks that third parties can present.

  Download the Guide to Third-Party Risk Management

- **Policy Management: Creating a Powerful Management System**
  Policy management can be an expensive, heavy burden on internal resources. Let's explore best-practice methods for not only reducing cost, but also developing great policies and efficient approval, distribution and training processes.

  Download the Guide to Policy Management

- **Incident Management: Beyond a Whistleblower Hotline**
  Providing a comprehensive, trusted and engaging process for employees to report unethical behavior is vital to the health of every organization. Read this guide to find out how to turn your incident management program into a world-class operation.

  Download the Guide to Incident Management

- **Compliance Program Assessment: Driving Value and Improvements**
  Effective compliance programs improve organizational culture, protect corporate reputation and enhance employee engagement. Download this guide for the best practice methods to elevate the effectiveness of your compliance program.

  Download the Guide to Program Assessment

compliance next™

Compliance Next gives professionals unlimited access to the best thinking in the industry. **It's free**, it only takes a minute to join, and it has the knowledge, resources, and expertise you've been looking for- all in one place. Join today, visit www.compliancenext.com.