ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

How to Use Risk Assessments to Shift Culture

Compliance and Ethics

CHEAT SHEET

- ***For the culture.*** The results of a solid risk assessment can help direct resources and improve culture. Beyond the need to do it for liability mitigation, organizations should seek to create and sustain an open and accountable culture, which helps create long-term value.
- ***Conducting an assessment.*** There is no “right way” to conduct a risk assessment. Your strategy should be tailored to the size of your organization, geographical scope, and your line of business. A great starting place is ensuring buy-in from upper management.
- ***Employee engagement.*** An employee engagement survey is one of the most powerful tools a company can use to gauge opinions regarding compliance. Asking employees for feedback will elicit whether any supervisor-led team is a risk for a compliance breach.
- ***In practice.*** When implemented effectively, risk assessments lead to data that can shine spotlights on potential vulnerabilities. Companies can turn this information into opportunities to reward honesty and build a sense of pride that will improve overall results.

Whether you have been in the compliance field for decades or you are brand new to the corporate world, there is no debating the critical nature of assessing your company's compliance risks. These assessments are, in fact, opportunities. With the right approach, they can go beyond simply protecting your organization and ultimately contribute to the culture you are trying to create. Sound lofty? Well, we have been in your shoes as current and former general counsel, and we have seen how risk assessments can be part of a cultural shift in ways both large and small.

You might as well approach risk assessments as opportunities — corporate counsel ignore the need for them at their own peril. In fact, with the new administration in Washington, DC, it is clear that compliance and enforcement will continue to be a focus for regulatory agencies. Take note, if you have not yet, of the US Department of Justice's (DOJ) Fraud Section's "Evaluation of Corporate Compliance Programs."[1] In this document, published in early 2017, the authors stress that the "Filip Factors," (taken from former Deputy Attorney General Mark Filip's 2008 memorandum regarding the Principles of Federal Prosecution of Business Organizations), while not to be applied in a rigidly formulaic manner, should be considered when assessing the effectiveness of a corporate compliance program.

These factors are considered in the context of an investigation into a corporate entity's potentially criminal activity and should include the "existence and effectiveness" of a corporation's compliance program as well as "remedial efforts 'to implement an effective corporate compliance program or to improve an existing one.'" When a breach has occurred, topics such as prior indications, the process for designing the compliance program, and risk assessment are front and center.

1 US Department of Justice, Criminal Division, Fraud Section: Evaluation of Corporate Compliance Programs. (PDF)

Imperative for the risk assessment

First, let's review the origins of compliance risk assessment. Risk management, or enterprise risk management (ERM), has received a great deal of attention in corporate circles and boardrooms. Enhanced frameworks have evolved into full-blown programs that assess several specific and high-profile risk areas that could derail a company from achieving its strategic objectives. These risks are identified, defined, categorized, and measured with detailed metrics to enable an executive management team to see around corners and ensure that risks are mitigated as they arise — and far before they turn from risk to event.

Oftentimes, compliance risk is only one risk silo identified and tracked with useful metrics. Overall, the enterprise compliance program is a mitigant to any compliance-related risk. The ERM program of risk assessment is very important for an organization, and compliance professionals should be linked professionally to their risk counterparts. ERM is not, however, a substitute for the compliance risk assessment.

The compliance risk assessment is meant to identify and categorize specific compliance risks. It is truly the foundation to plan your enterprise compliance program. If done correctly, it can identify weaknesses and lead to adjustments in your communication, training, and auditing programs. Even better, it should be used to set your compliance culture — and can even be used to set a cultural tone for an organization of openness, honesty, and accountability.

The risk assessment was formally included in the Federal Sentencing Guidelines when they were

amended in 2004.[2] The guidelines outlined the necessary mechanics of a compliance program, underscoring the need for a benefit or credit that leads to a reduction in an organization's culpability. In the text, the inclusion of a periodic risk assessment was noticed throughout corporate America. The Federal Sentencing Guidelines' language sets the risk assessment as the predicate to program design and any modifications thereto:

"The organization shall periodically assess the risk of criminal conduct and shall take appropriate steps to design, implement, or modify … [the program] to reduce the risk of criminal conduct identified through this process."[3]

2 US Sentencing Commission, Guidelines Manual §8B2.1(c)(2004).

3 Id.

While the language of the guidelines limits the assessment to criminal conduct, because many federal agencies have adopted the framework for their own enforcement program, the compliance risk assessment has been broadened beyond criminal risk. Typical areas covered by a compliance risk assessment include criminal, regulatory, ethical, and other spaces.

The DOJ memo has several risk assessment areas of inquiry: questions probe the process; the methodology used to identify, analyze, and address a particular risk; and the information gathering and analysis to assess the risk, including information or metrics that the company has collected to help detect the type of misconduct that has occurred, how the metrics inform the compliance program, and how the risk assessment process accounts for risks that have actually manifested themselves. Moreover, it seeks to know about risk-based training and continuous improvement. All of these are areas that should be covered by the risk assessment and reported annually to the board.

Most importantly, however, the results of a solid risk assessment and how that information is used can prove the compliance function has strategic value. The risk assessment can help direct resources and improve culture. Far beyond the need to do it for liability mitigation, organizations should want to do it to create and sustain an open and accountable culture, which in turn helps to create and sustain long-term value in the organization as a whole.

For publicly-traded companies, think about how quickly other listed companies' values have dropped because of a fraud or crisis. BP's stock value dropped by more than 50 percent after the Deepwater Horizon spill; Enron's value never returned, as it went entirely insolvent and dissolved as an entity. We don't want to overstate it, but your risk assessment — if also used as a cultural tool — can truly be a crisis averted.

Tone at the top

Now, let's focus on the importance of culture and tone at the top, middle, and frontline.

How does this relate to a tactical project like a risk assessment? It is imperative that the leadership within an organization, at every level, supports an open and honest culture: One where individual employees have the ability to speak and voice concerns with faith and confidence that they will not be compromised in any way. A risk assessment, at its base, is a tool to listen to your employees. If they believe they cannot, without fear of retaliation, identify a risk or express a concern about a risk area, the results of your assessment will not hold value. Worse, you will have lost one of the best opportunities to uncover compliance shortcomings. Conversely, once you convince them that it is

safe to speak up and that their opinions will help create a roadmap toward effective compliance programs, you will learn your true vulnerabilities.

C-suite executives, along with the board, hold the ultimate responsibility for culture and tone at the top. Yet, it is really the frontline managers who can make or break your culture. If you believe you have management risks, address them in how your risk assessment is designed, and then address them with your organizational development team. If you are in a multi-year compliance program building phase, it is a great idea to work hand-in-glove with your organizational development or human resources team to assess culture, fear of retaliation, trust in superiors, and the like. Time and again, we have found that where there are frontline leaders who are not trusted, there is also a high risk for compliance breaches.

Conducting the risk assessment

Tactically, there are several ways — and no one right way — to conduct your risk assessment.[4] Your strategy should be tailored to the size of your organization, your geographical breadth, and your line of business. In light of the tone at the top discussion, a great starting place is to ensure you have the buy-in of upper management. A 15-minute discussion with them about what you are doing and why, with a specific request that they support the initiative with their teams, will pay dividends in terms of the time and attention given to the risk assessment by the employee base.

Surveying or interviewing lead employees in person also provides a great base for your risk assessment.[5] Hopefully, you have a well-constructed compliance program manual that identifies lead employees responsible for compliance over areas such as corruption and risk, anti-bribery, antitrust, export, environmental, harassment and discrimination, specific federal regulatory bodies, third-party and joint-venture risk, M&A — you get the picture. If you do not, take a look at your organizational flow chart and identify the key people in those areas, as well as others that have a compliance need associated with them. Ask them targeted questions: What could go wrong? Where are the holes? How do they train? What would be the impact of a compliance breach? If your organization is too large or geographically diverse for in-person interviews, written surveys through an online service are another way to perform this function. Be certain, however, to get on the telephone and follow up with those folks who either do not respond or who provide you with answers that require further exploration.

4 A great starting place for how to conduct a risk assessment is found in the Society of Corporate Compliance and Ethics, Complete Compliance and Ethics Manual, Chapter 3. 363 (2017).

5 This article does not address attorney-client privilege issues around risk assessments. We strongly advise, however, that you conduct these interviews and your risk assessment in such a way so as to protect the attorney-client privilege, or at least the assertion of it.

You can get very numbers oriented, asking people to assign numerical values to the risk of a breach and the impact of that breach, or you can listen to the stories you hear in your interviews — or both. At the end of the day, your goal is to be able to assess the risk associated with each area individually. The risks do not have to be ranked. Although with everything in life, you will want to determine which ones are highest priority: Those risks most likely to occur and with the largest impact to the business deserve your sharpest focus. It is important that you have identified other risks as well. In fact, many companies smartly say they have zero tolerance for any compliance violations. In this context, the impact of a compliance risk turning to a compliance breach matters regardless of the impact.

You should not stop there, however. As we noted, with the advent of ERM programs, there is a stronger knowledge base among your colleagues than ever before. Take your initial findings from your risk assessment and then pressure test them with your ERM, internal audit, and chief risk officer counterparts. They are also seeking out risk identification and may have uncovered a risk that your own risk assessment missed. From the US Sarbanes-Oxley Act internal controls to the fraud risk assessment, to other strategic risks, your colleagues are probing business vulnerabilities and, in our experience, are uncovering compliance risks as they do so. Share your assessment with them and incorporate their findings into your own body of knowledge.

This knowledge base allows you to structure your communication and training plan, understand how best to allocate your resources, how to design remediation and mitigation, where to point compliance audits, and how to create incentives for employees to do the right thing through full compliance with the laws, regulations, and policies.

Resources to conduct a risk assessment:

- Association of Corporate Counsel (ACC). ACC offers sample risk assessment templates and a variety of other resources to its 40,000 members around the globe.
- Society of Corporate Compliance and Ethics (SCCE). The SCCE provides training, certification, networking, and other resources to its members, who include compliance officers and staff from a wide range of industries.
- National Association of Corporate Directors (NACD). The NACD has an online resource center focused on risk oversight, which includes practical guidance and tools for boards, committees, and individual directors.
- Association of Certified Fraud Examines (ACFE). The ACFE has an online fraud risk assessment tool to help its members identify and address vulnerabilities related to internal fraud.

Risk assessment as a cultural tool

So, the nuts and bolts of a risk assessment are fairly straightforward. Now, how to explain the cultural shifts that a risk assessment can create? Let us start by owning the fact that we view a self-governing culture to be the aspiration. We have both been part of a highly regulated and highly safety-conscious industry that relies heavily on our employees' shared values that motivate them to protect each other, the community, and our companies' reputations.[6]

6 For a good read on this concept, we recommend Dov Seidman's *How: Why How We Do Anything Means Everything* (2007).

Accordingly, it is all in your approach and relationships. Communication on the importance of compliance is paramount, but you must figure out a way to go beyond a you shall comply" commandment. A risk assessment can allow you the face time with the key players in your company. Leaders need to know why compliance is important, why a regulation is in place, and most certainly why it matters to the company. Headlines are an eye-catcher. Most employees at every level understand the implications of a negative headline on the business and eventually on their paychecks, even their jobs.

Beyond the scare tactics, however, people genuinely want to like and respect their workplace. If you can create a work environment that is respectful and trustworthy, people will want to be there — and they will want to protect it. If a manager can explain the “why” behind a policy, it can gain more traction through understanding.

Additionally, asking your employees to focus on compliance risks to the organization enables them to consider the impact of their decisions from the lens of the compliance team. You want them to be thinking about the answers to open-ended questions such as:

- What is the single greatest risk facing the organization today?
- What is the single greatest risk for you to meet your legal obligations?
- What is keeping you up at night?
- How do you know you are fully compliant?
- What roadblocks exist for you to stay compliant?
- Where do you go for expert answers?
- Who is responsible for ensuring compliance in your area?
- When do you focus on your compliance obligations?

One of the most powerful pieces a company can utilize is an employee engagement survey. That too can be a part of your periodic risk assessment. Work with your colleagues who lead that effort and ask them to add questions that assess your compliance culture — risks will be drawn out. Asking employees feedback to statements such as “I can trust my supervisor;” “I can report a concern without fear of retaliation;” “I understand my role in complying with rules and regulations;” and “my supervisor is honest” will all elicit whether any supervisor-led team is a risk in itself for a compliance breach.

Generally, engagement surveys should drill into the data by supervisor in order to assess the health of the team. If one specific leader seems to have employees that respond in a negative way to the statements we pose above, it is imperative that the compliance team dig deeper. We share a story below that emphasizes this point.

A risk assessment in practice

A number of years ago, one of our teams decided it was time for an in-person training combining compliance and risk assessment. We set out to get face-to-face with 1,900 employees in a six-month time period — no small task. But we did so because through past risk assessments and other cultural surveys, we were concerned that we may not be hearing everything we needed to and that employees were not fully grasping compliance as a program.

Most illuminating was the reaction when we asked a group of employees, “Are you proud to work here?” They were, and they told us why. A pillar of the community, a way to give back, and a means by which to put children through college all were themes that rose up in these conversations. In that context, compliance risks were relevant. If a breach means that any of that is in jeopardy, then one person’s actions can affect the whole. That is when you create a program that matters, because people will speak up and tell someone if a compliance breach has happened, is about to happen, or if there is a concern at some level.

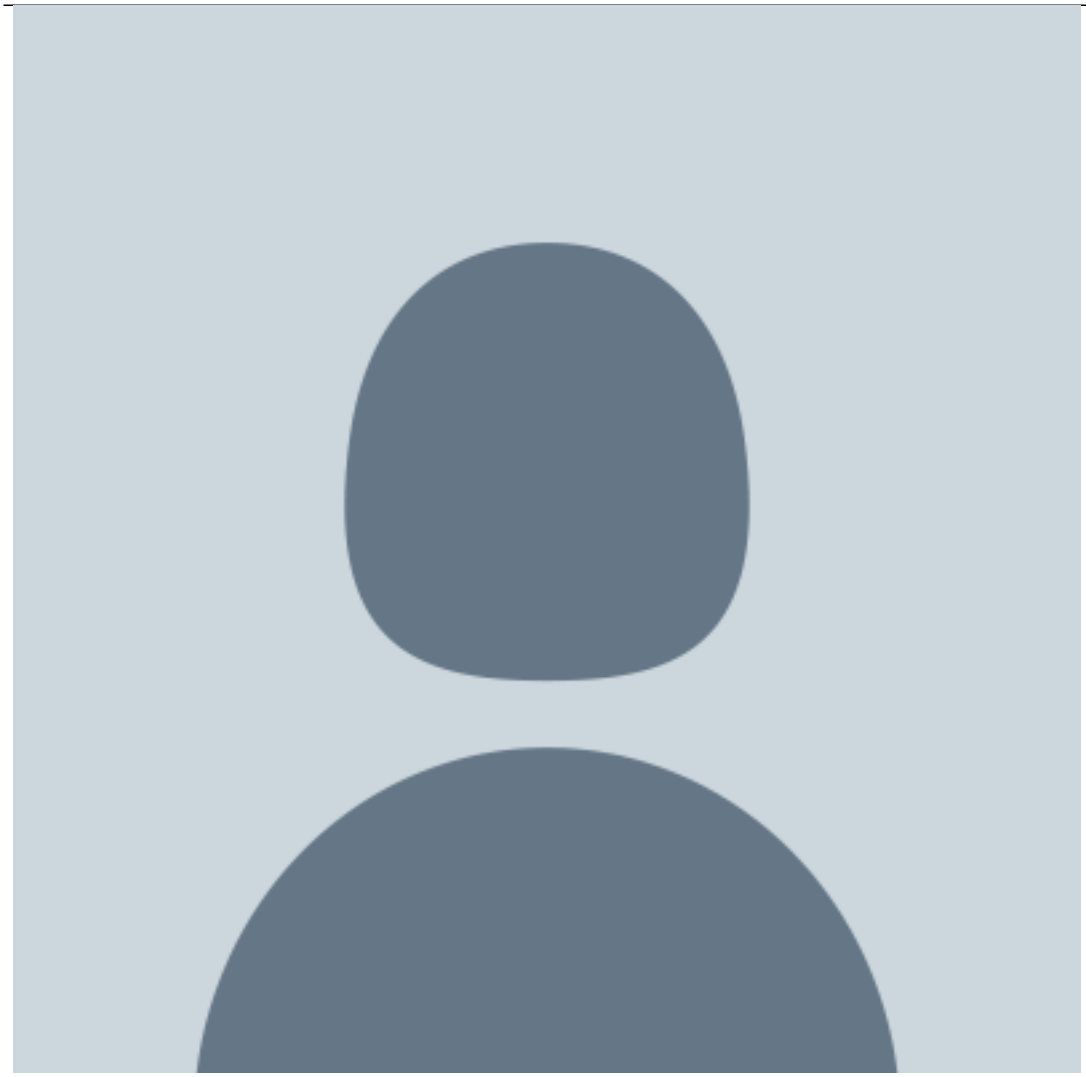
For us, the compliance concerns centered on conflicts of interest and the gifts policy. Employees were uncertain of the full parameters but knew they did not want to unwittingly breach it. We were able to address their questions, offer concrete examples, and tailor training for the rest of the

workforce focused on conflicts and gifts. It was heartening to know that employees' motivation was true — they desired to comply. We quickly realized our job was to make it easy for them to do so.

Another case relates to the use of employee engagement survey data as part of your risk assessment, if that makes sense for your organization. One of us was able to host communication meetings with small groups of employees whose team survey results indicated a cultural breakdown when it came to compliance. Further communication with the team uncovered an unhealthy leader that was behaving in ways that put the organization at risk. However, the company was able to get ahead of it before it arose to the level of fraud, and then was able to build a team that became one of the healthiest and most engaged across the entire organization.

Those examples prove the point that the risk assessment process can help shift your compliance culture. When designed and implemented effectively, risk assessments lead to data that shine spotlights on potential vulnerabilities. When they are acted on immediately, companies can turn those vulnerabilities into opportunities to reward honesty, build trust and accountability, create a sense of pride, and improve your overall business. That is our fundamental point: Compliance done right leads to strategic results.

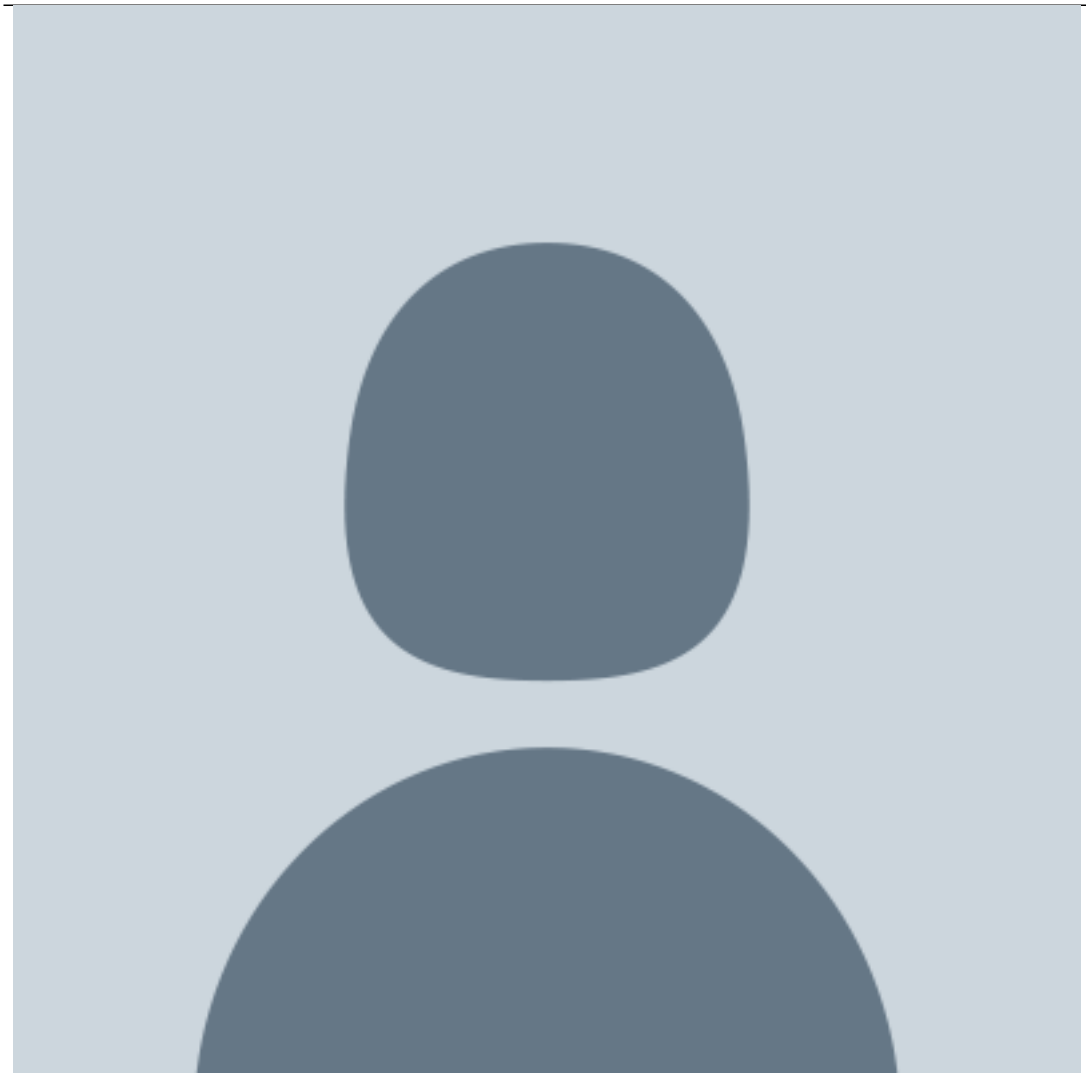
Karen Haller



Senior Vice President, General Counsel, and Corporate Secretary

Southwest Gas Corporation

Jane Lewis-Raymonds



Co-Leader

Parker Poe’s Governance, Risk & Compliance group

She is a member of its Energy group. With more than 25 years of legal experience, including a decade as GC and CCO of a publicly traded company, she has significant depth of knowledge relating to all aspects of corporate law, including enterprise compliance, securities, public company legal and governance issues, as well as board oversight of cybersecurity, crisis, and risk management.