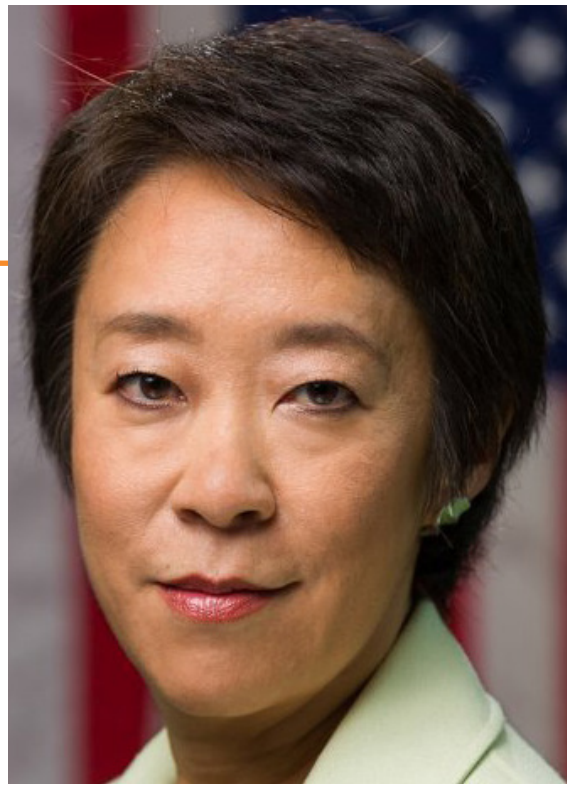
INDUSTRY EXPERT HUI CHEN ON

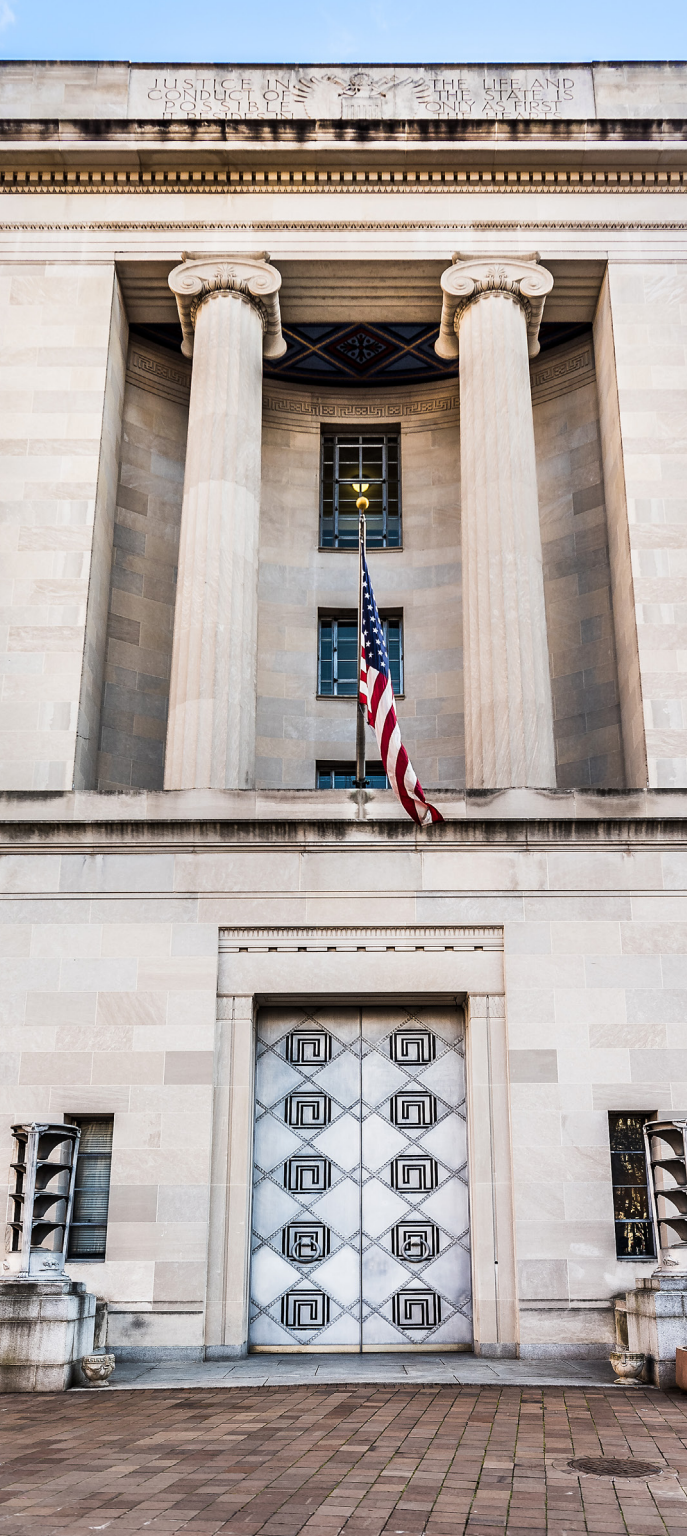
ETHICS & COMPLIANCE

HUI CHEN



As the first-ever Compliance Counsel Expert at the United States Department of Justice (DOJ), Hui Chen served as exclusive consultant to the Fraud Section's white-collar crime federal prosecutors. She reviewed corporate ethics & compliance programs for companies in areas such as anti-fraud, anti-bribery/ kickback, healthcare, quality control, manipulation of financial markets, process safety and environmental protection. She also authored the Fraud Section's "Evaluation of Corporate Compliance," a publication praised by compliance practitioners, government regulators and standard setters around the world.

Recently, Mitratech's VP of Business Development, Jason Cropper, sat down with Chen to discuss her work at the DOJ, her advice for creating and maintaining a culture of compliance, and her insight into how technology can serve as a tool in this arena.



Tell us a little about your experience at the DOJ. What was your role and how did your time there inform your perspective on compliance and anti-corruption?

I was at the DOJ from late 2015 to the end of June 2017. Prior to that I held a number of in-house positions at Microsoft, Pfizer and Standard Chartered Bank. I am currently an independent ethics and compliance consultant.

At the DOJ, my role was to serve as expert consultant to the prosecutors in the Fraud Section of the Criminal Division. The Fraud Section specializes in the prosecution of complex white-collar crimes in three specific areas as represented by three litigating units: the Foreign Corrupt Practices Act Unit, the Securities and Financial Fraud Unit and the Health Care Fraud Unit. All three units of the Fraud Section prosecute corporations as well as individuals.

When they prosecute corporations, DOJ policy mandates that the prosecutors consider certain factors relevant to the corporation's conduct called Filip Factors. Out of the ten Filip Factors, two focus on compliance. The first measures the existence and effectiveness of the company's pre-existing compliance program from before the misconduct occurred. The other factor is remediation.

Remediation can mean what actions the company took to discipline the employees engaged in the misconduct, whether the company compensated the victims impacted by the misconduct and whether the company enhanced their compliance program as a result of the misconduct.

I worked with prosecutors to evaluate the companies' Filip Factors as they considered what charges to bring and the appropriate resolutions. My specific focus was to assist them on the evaluation of the two compliance related components of the Filip Factors. In a nutshell, that was the main part of my work with the Fraud Section.

As a result of a resolution with the Fraud Section, companies can either be placed under monitor-ship or they can self-report their progress on enhancing their compliance programs. Whether they self-reported or were monitored, I worked with either the company to review the progress they made or with

the monitor to ensure that companies comply with the terms of resolution.

Because of my background and experience with the DOJ, I have a unique perspective on compliance. I have seen what really works and what doesn't in all kinds of compliance programs.

When people talk about compliance, they tend to think about the Foreign Corruption Protection Act (FCPA), but compliance is more diverse than that. I've been involved in everything from anti-corruption to Health and Safety compliance, including working with monitors on the 2010 BP oil spill disaster to the criminal prosecutions resulting from quality issues at Volkswagen and Takata.

What's unique about my approach is that I look at compliance from an integrated perspective. Many companies compartmentalize their compliance, such as anti-corruption, sexual harassment, health and safety, etc. I believe companies should approach these different types of compliance in a more integrated manner based on an appeal to the employees' value systems.

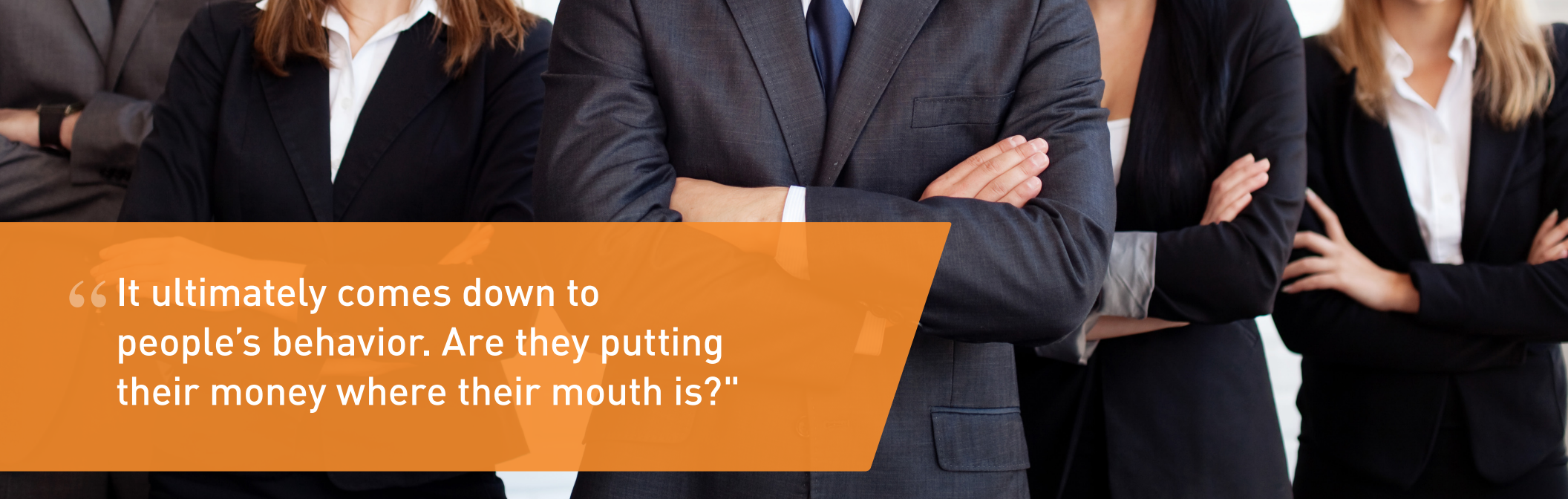
Another unique perspective I bring is my focus on measuring data. This is something relatively new that has very much influenced my work - specifically in terms of how a robust compliance program can be measured and proven. I'm focused on how data can be used to understand risk and potential risk, and how it can be used as evidence to measure the effectiveness of a compliance program.

Can you provide more insight into what creates a culture of compliance and how senior management can demonstrate or measure this culture?

This is an interesting question. In my daily life as a compliance person, I ask people how they know if their manager or senior management is committed to compliance. Many people respond with "My manager really cares about this because he's always asking me about it," or "I always know my manager cares about this because he's constantly checking to make sure we do this right." They hardly ever cite the things their managers say, rather they cite the things they do. These are examples of management making a choice to pay attention to something.

Ultimately, it comes down to behavior. Is management leading by example? Are they putting their time, money and action where

"I'm focused on how data can be used to understand risk and potential risk, and how it can be used as evidence to measure the effectiveness of a compliance program."



> “It ultimately comes down to people’s behavior. Are they putting their money where their mouth is?"

their mouth is? For example, if you have an interview with a company for a compliance officer position, how do you know the company is really committed to what they say they want you to do? When you pause and think about it, it all comes down to the choices that are made, how time is spent and how resources are allocated. These answers are what ultimately convince you of a manager’s or company’s commitment—not what they say.

In the anti-corruption compliance community, there’s a belief that we don’t know how to measure culture. However, many people cite the Transparency International Corruption Perception index, which is a type of perception measurement. It’s interesting that people say they don’t know how to measure culture, yet they’re actively using this metric without thinking about the specifics. If you can measure a whole country’s perception, why can’t you measure a company’s perception?

Continuing on the topic of creating a culture of compliance, many people advocate a top-down approach. However, embedding that culture into all levels of the organization can be challenging at best. Sometimes, there’s a perception that the top-down approach is simply a “tick-box” exercise. What’s your view on this?

I think the best top-down approach to a culture of compliance is starting with a bottom-up approach. When I say that, I mean that if a top-down approach does not reflect the values of your employees and stakeholders, it can only go so far. A truly effective top-down approach is a reflection of the values of all the stakeholders involved. In order to know what those values are, you have to start with a bottom-up approach.

How do you measure the effectiveness of a compliance program? What types of questions should organizations ask themselves when in the process of building an effective program?

What I look for is a form of measurement to back the adjectives people tend to use. For example, if a company states they have a robust compliance tone at the top, yet a survey indicates a significant number of employees believe they will be retaliated against if they raise an issue, then the measurement doesn't back up the claim. Often, when companies talk about a robust tone, they are just using the wrong metrics and measuring the wrong things, such as simply the number of communications.

There are a number of ways to measure tone from the top. When you just measure the number of times someone says something pro-compliance, that measurement doesn't present the full picture. Are you also measuring how often the same people send messages that may be contrary to compliance and comparing the two numbers?

Finally, how is your commitment actually received? It's not about what you sputter out, it's about what people actually believe and I don't see anyone measuring that.

Another example of people counting the wrong numbers is in training. I've had many conversations with people who have been counting completion rates as a measure of the success of a training program. They're measuring effectiveness by the number of training completions.

Now, if you're a company that rewards people with promotion simply because they show up at their job every day, then go ahead—that would be consistent with your values. But I don't know of any company that awards promotions purely because somebody showed up for work. They need to demonstrate that they do good work, so why is the same not true when you're measuring training?

People often ask me what they should measure in training and my response is for them to tell me what the purpose or goal of their training is. What exactly do you want your training to accomplish?

I have to force people to be honest with themselves and tell them that if their goal of training is to simply show that people participated in the training, then yes, completion rates are the measure. But if your goal is actually to get people to understand a certain process, then you need to measure how they're doing in terms of that process. For example, if you're rolling out a new set of approval systems, you should measure how the people are following that system before the training versus six months after the training.

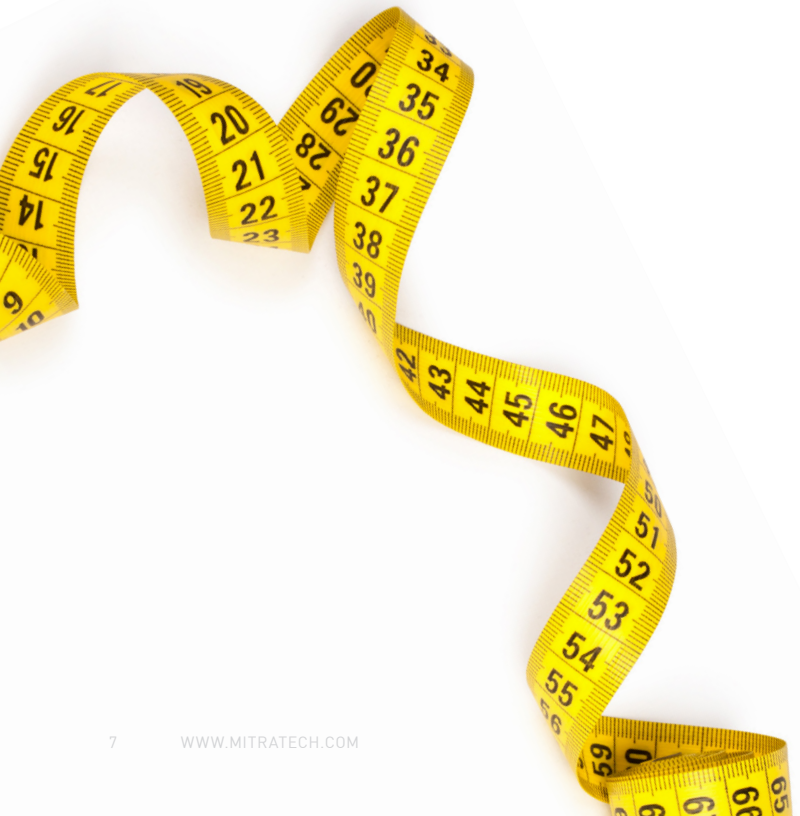
After you roll out a policy, what are you hoping to accomplish with that policy? What is the purpose of that policy? I think it goes back to the "why" question. Why are you doing this training? If your training is successful what would be the result? I don't think people are asking the "why" question enough.

Having employees who are simply more knowledgeable about something is not necessarily the goal of training, because what does pure knowledge do? What you're ultimately hoping to do is change behavior.

For example, why would you want to turn your employees into experts on anti-trust or UK Bribery Act? What you actually want is for them not to take a bribe, not to give a bribe, and to raise their hand if they see something that needs to be reported.

You don't need them to understand the difference between passive and active bribes or what the name of the statute involved is. It's not so much about knowledge, but more about behavior.

> "The problem is not with knowledge. The problem is with behavior. You should be measuring behavior."



I have rarely met anybody who engaged in misconduct that honestly did not know what they were doing was wrong. The problem is not with knowledge. The problem is with behavior. You should be measuring behavior.

Many people look to published guidelines for insight into what makes an effective compliance program. Some say, "These are just guidelines, so we'll take the risk rather than invest in an effective program." Do you have any thoughts on this line of thinking?

I think the problem is that there are too many guidelines. Again, every important agency I have mentioned has a variety of guidelines. Which guidelines are you going to look at first? That's just U.S. federal and state. I can probably come up with a hundred agencies that have some kind of guidelines relating to some form of compliance. You multiply that with different jurisdictions outside the U.S. and now you're talking hundreds of guidelines. Whose guidelines are you going to follow and in what area?

If you're just chasing everyone else's guideline, you will always be chasing. In fact, in some areas, you probably run into conflicting guidelines. A lot of people struggle with this, particularly in areas of compliance that are not so value-based, such as data privacy and record keeping.

These fields are very regulatory in nature. Some jurisdictions say you may not keep data for more than five years while others say you may not keep data for less than five years. So what do you do?

When looking at the various areas of effectiveness, what does the DOJ look for in terms of remediation and continuous improvement?

There are several ways to look at this. In the context of the DOJ's evaluation of compliance programs, those questions apply to a very specific set of circumstances. For example, if the company is under criminal investigation for a specific set of conduct. That's where everything begins because the DOJ would not be sitting across the table from you asking about your compliance program if there wasn't something that already went wrong in the first place. If you're talking to the DOJ for an anti-trust violation, they're not going to ask you about your health and safety.

The remediation, root cause analysis and continuous improvement all serve one purpose: to ensure that you

don't keep making the same mistakes and to prevent any recurrence of issues.

Every time something goes wrong, you should sit down and figure out why it went wrong. What in the system allowed it to go wrong? People often ask me about rogue employees. They ask if I believe there are situations where there just might be a rogue employee.

My answer is yes, of course. However, the compelling questions they should be asking are why did the employee go rogue in your organization at this time in this place in this way? How was he or she enabled in going rogue? Sometimes in some companies it's very easy to go rogue. In other companies it's much more difficult. I want to know what is it about your system that enabled this behavior. What in your process went wrong?

Every time something goes wrong, you can learn from it, even in situations that aren't that significant. To share my favorite example, let's say you have an approval system that somebody violated and the first time, when they failed to get approval, it was no big deal. It was something that they would have gotten approval for anyway had they gone through the approval process. Most companies I know would say, "Oh, no harm no foul. Let's just move on." But the next time you may not be so lucky. Next time, when somebody evades that system it could be for something truly detrimental. What you want to do is think about why this control failed. Is it because the control is too burdensome? Is it because the person didn't know about it? Whenever something goes wrong, if you can engage in that kind of self-reflection as an organization, I think that's what drives the continuous improvement in your system. Everything you're doing needs to back into how your system works and how you continually reflect.

Let's talk about risk assessment. How do risk assessments tie into an effective compliance program and what do you look for there?

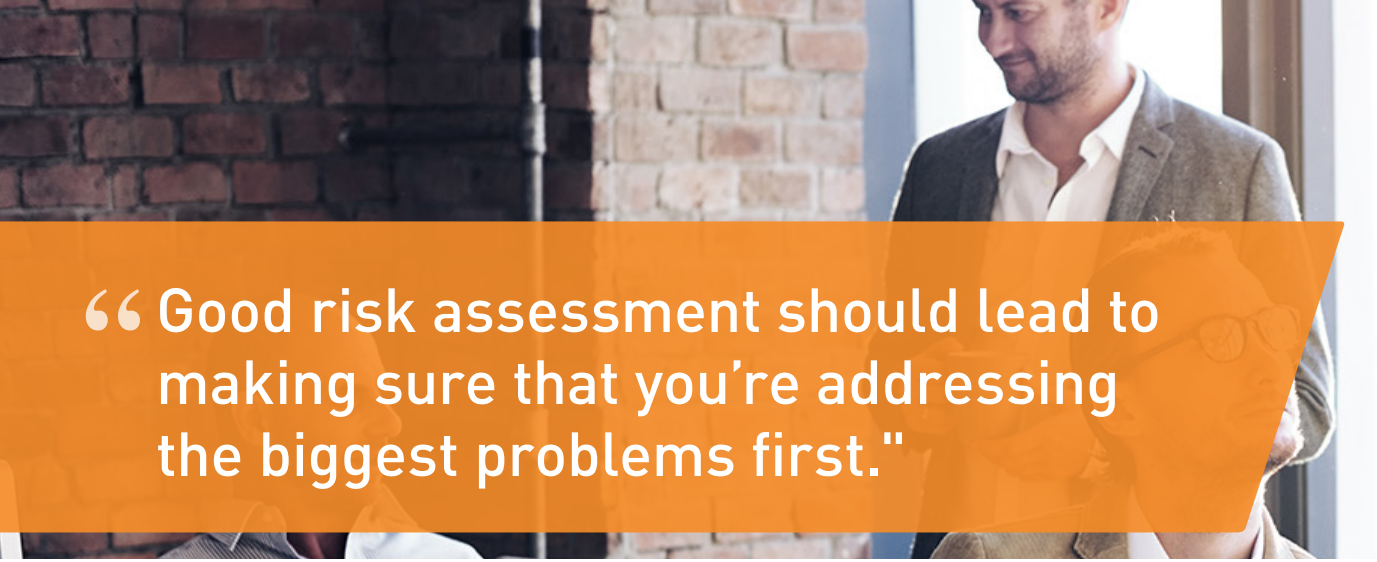
One of the things I always ask when I'm meeting with companies and compliance officers is, "Can you give me an assessment of your company's risk profile in this particular area of risk?" Half the time compliance officers are not able to answer that question, which is truly concerning. If you don't even know what the risks are how are you supposed to address them?

Part of risk assessment is making sure you address the biggest problems first. Are you allocating your resources—whether it's time, money or control systems—in a way that's proportionate to the potential damages it could cause?

I've encountered many companies that immediately focus on gifts and entertainment in anti-bribery and corruption compliance. I ask them how much their gifts and entertainment represent in terms of the company's total spend. I don't believe I have ever encountered a company where gifts and entertainment was their biggest category of spend. It's usually some form of third party spend that needs to be broken down such as suppliers, margins, discounts, etc., that are granted to their distributors or sales agents.

I learned that lesson very early in my first compliance job with Microsoft. I remember talking to the chief financial officer of the organization I was working with and he said, "Look, everybody's focused on gifts and entertainment, and that's maybe a few hundred or a few thousand dollars. I'm focused on discounts and margins. Those are millions of dollars."

That was my early lesson in learning about where to focus. Another example is in health and safety compliance – you need to focus on whose safety is most at risk. If you're an oil company and you're more focused



> “Good risk assessment should lead to making sure that you’re addressing the biggest problems first."

on office workers than rig workers then you have a problem. You’re not focusing on the people who are most at risk. Good risk assessment should lead to making sure that you’re addressing the biggest problems first.

When we look into the world of enforcement, we see many organizations concentrating on the Foreign Corrupt Practices Act (FCPA). Is the FCPA the most enforced area or are there other areas as well?

Not at all. It is so puzzling to me why FCPA compliance is so prominent in the compliance community almost to the point of obscuring everything else. If you look at the Fraud Section’s annual reports over the last two years, the Financial Securities Fraud unit has brought in more guilty pleas and penalties than the FCPA unit in terms of dollar amounts and guilty pleas.

I don’t understand why people aren’t focused on cheating in emission controls or exploding airbags. Agencies like the Consumer Fraud Protection Bureau have engaged in many, many more enforcement actions than the FCPA. Why doesn’t that get any attention in the compliance blogosphere?

What about domestic bribery? We can’t ignore the fact that United Airlines bribed the chairman of the Port Authority in New Jersey, yet this received almost no mention in the compliance circle.

The enforcement is there. If you look at the Environmental Protection Agency, it has a very active enforcement program even though it’s facing many challenges under the current administration. Why doesn’t the compliance community pay more attention to environmental enforcement?

This is the problem. There are hundreds of enforcement agencies between federal and state. Why is everybody just focused on the Fraud Section? Why are we not looking at the Consumer Fraud Protection Bureau? Why are we not looking at the Federal Communications Commission and the Federal Trade Commission and the Securities and Exchange Commission (SEC)? You get some attention with the SEC, but again only with their FCPA cases. They do lots of other cases too.

I think FCPA enforcement has gotten an utterly

disproportionate amount of attention in the compliance community. I do not think that's the majority of enforcement at all. Again, let's go back to the data. We should look at data and examine what areas companies have paid the most fines and penalties in. I would wager that it is not the FCPA. It's not even close.

It's clear that there has been a rise in a need for compliance and risk technology. How do you think technology is helping this field? How do you think technology can help analyze and demonstrate the effectiveness of a compliance program?

As with any tool, the effectiveness of technology depends on how people are using it. When understood and used as a tool, technology can be enormously useful. However, if you use technology as a substitute for judgment and your brain then it actually hurts.

One area where technology would be helpful is its ability to aggregate data. Again, keep in mind how you use the tool. I recently heard a story of how people can manipulate both data and technologies. For example, let's say you have a chief compliance officer who says, "Our investigations take too long. The system is calculating that our investigations take an average of 45 days. Let's make it a goal that we reduce our investigation cycle times to 30 days."

Sure enough, next quarter, investigation cycle times drop to 30 days. How did that happen? When you walk around and talk to people, you find out they are not actually doing anything differently. They just tweaked the system to change the definition of when a matter is closed or open. The system measures the days and that's great. However, the system can be tweaked to change how it calculates. Now you have an artificial drop in the investigation cycle times.

The important questions to ask when using technology to understand metrics and data are always 'why' and 'how?' How have you come to this?

I spoke earlier about the importance of asking 'why,' but what about 'how'? If you present a certain measurement, whether it's arrived at through the use of technology or not, we're going to ask how you did that. The devil is often in the details.

I do think that technology offers the ability to make certain processes easier. If you want people to behave a certain way, it helps to make that behavior an easier choice to make. Technology has the ability to aggregate data. It also has the ability to make certain steps easier for people to follow. For example, I have seen companies make good apps for employees to use for certain approval flows, which makes it easier for people to follow the process. However, you always want to make sure technology doesn't just become a process without a brain behind it.

At Mitratech, we sometimes receive feedback from companies who would love to invest in this technology, but state they don't have the resources or budget to do it. At what point is it appropriate for a company to invest in compliance technology to help them meet their needs as a business?

As an organization, you have to look at a number of factors. First, look at how your spending in this area compares to your spending in other areas.

For example, years ago my friend's husband was a healthcare consultant. My friend told me that when they went to some pharmaceutical conferences, she would come back to their hotel every night and find lavish gifts on the pillow. If you're going to spend that much money on your conferences, yet in contrast you're only spending $20,000 on your annual compliance budget, then I would think there's a problem. In this case, your company clearly has the money, yet you are choosing to spend it on something else.

I've seen companies that, when you look at their overall investment in resources, compliance-related function is clearly the red-headed stepchild in the room. Everybody else received generous budgets and head counts compared to compliance, or audit or some other department.

That's one way to look at how reasonable your choices are. The other way is to also look at how smart your choices are. I have seen companies that come into the Justice Department after they get into trouble. As a result, they spend a disproportionate amount of money on compliance in a way that's really not necessary for their organization. In those cases, you wonder if these companies are just doing it to show us for now, because this is clearly not going to be sustainable in some organizations. An organization cannot support an over-bloated type of program of any kind.

Let's say there's a technology that could help you deliver training in a more focused way, such as training that helps you focus on the employee population who are either at risk or working in control functions. In some cases, companies are not calculating the cost appropriately. When you do a training that's completely irrelevant to somebody's job, you waste your employee's time. You need to think about the average pay of your employee and add that number up per hour for your training. I bet you that's a significant amount of money.

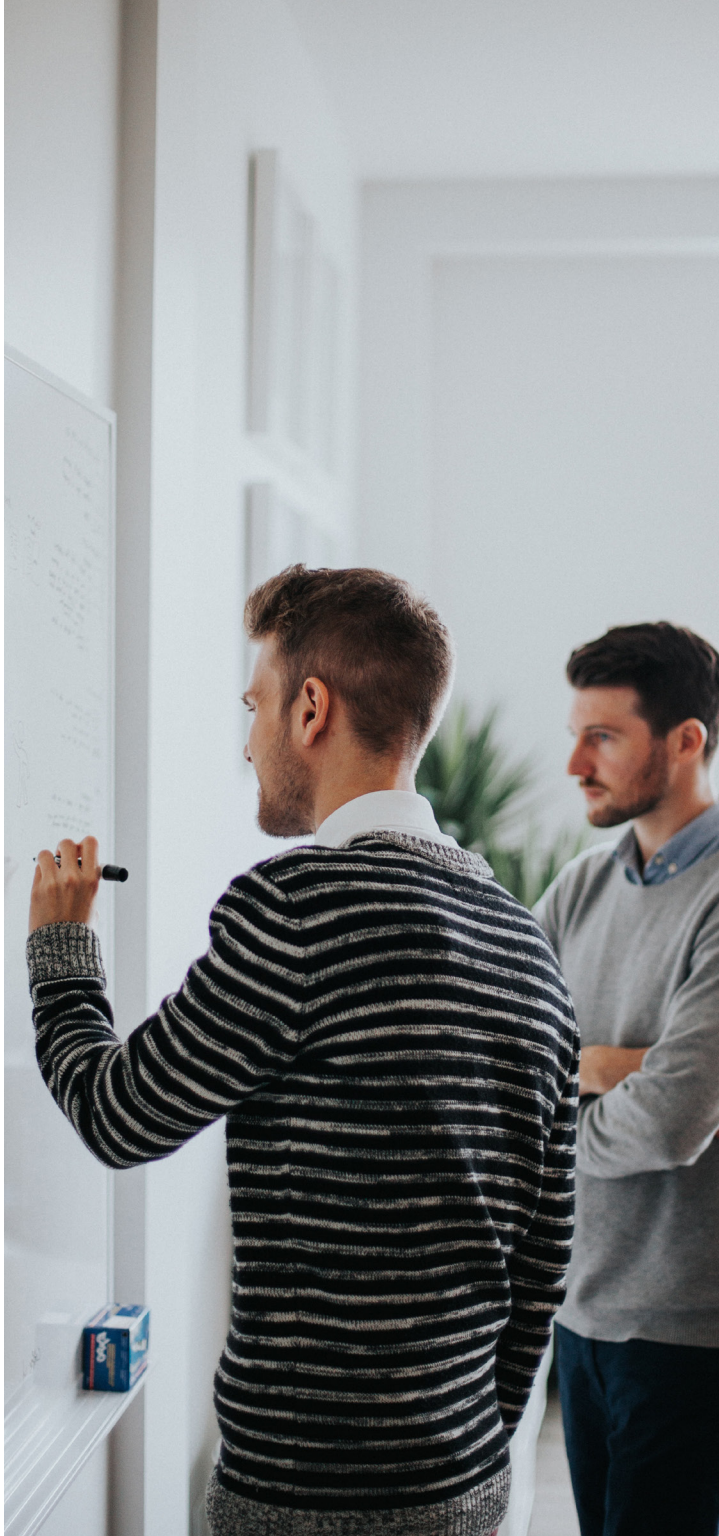
What is the legal department's role—and what should it be—in the area of compliance?

This is a popular area of discussion. I don't believe in any kind of fixed model and I'm not going to hold out a model and say this is the model that works.

One important area to understand is to what extent the compliance function is independent. I think that is an important area because compliance may have different interests than legal at times.

Legal, by definition, may be more interested in protecting the organization. Sometimes that protection may be interpreted as, "We don't want to know too much." Whereas compliance always wants to know more. A good compliance function wants to know what happened, how to fix things based on what you learn about what happened and what are the system weaknesses.

In some ways, that may present a conflict. The question is how is that potential conflict handled? Is compliance able to speak up and do what it needs to



do with reasonable business sensitivities, in spite of the potential conflict with the legal department's interest in that area?

Because compliance in the United States has often been associated with legal, and is often run by people with legal training, that could be where some of the lack of data focus and "tick-box" mentality comes from. When you conflate compliance with legal interest, your first reaction is to see what the legal requirement is and to meet it, as opposed to what the actual risk is and to manage it. I think that may have created a mindset that's led us to where we are.

Legal folks, and I speak for myself as someone trained as a lawyer, don't tend to be very data driven or focused on numbers. I realize that's a generalization. I will say I've always wanted to be a lawyer, but one of the reasons I can't be something else is because I'm not good at math. The data focus is something that's not an inherent part of the legal skill set and that may have led to some of the approaches that are prevailing in compliance in the U.S. today.

A data-driven focus is something that could really benefit legal, and not just from a compliance perspective. Legal as a whole could benefit from it because ultimately, you need to remember that when you're working, whether it's legal or compliance or something else, you are serving a business entity. That entity is very revenue, ROI and KPI focused. Everybody is bringing some form of measurement to the table, and if you are the only function that can't bring measurement to the table, then you're already not speaking everyone else's language.

If we can analyze where our legal spend is going in terms of risk and compliance opportunities, then we can connect the dots between functions. Now that we see the bigger picture, how do we not only reduce our legal spend, but know where the spend is coming from? Can we work closer with compliance and risk to reduce our legal spend?

Yes, I can definitely see that. Legal spend, just like any other spend, should be subject to analysis and scrutiny, and often it's not.

It's funny, because when I've worked with law firms, they don't see themselves as a high risk industry, but they are extremely high risk. It's also interesting that legal spend is often based on perceived quality and not just pricing alone. Why did you go with this outside counsel or this outside accounting firm when there are obviously cheaper options available? It's an area of spend where judgment weighs a lot. As far as I know, no company picks an outside law firm based purely on how much they cost. This is an area where it's important for them to justify. They need to justify why they are spending all of this money on outside counsel in this area or on five different sets of outside counsel. How are they all different? Why are they paying all these fees?

As companies become more and more careful about how they spend their money, the legal function also needs to be responsive to that concern. Justifying their spending through measurement and supporting data would be extremely helpful in that regard.

Do you have any general words of wisdom or advice that you would give anyone from the compliance world?

I would say— Always think about why you are doing what you're doing. Think about how to measure success. Once you have the why, think about how to measure what success would look like.

MITRATECH

WWW.MITRATECH.COM

More About Hui Chen

As the first-ever Compliance Counsel Expert at the United States Department of Justice, Hui was the exclusive consultant to the white-collar federal prosecutors in the Fraud Section, reviewing corporate ethics and compliance programs of companies in areas such as anti-fraud, anti-bribery/kickback, healthcare, quality control, manipulation of financial markets, process safety, and environmental protection. She worked on landmark cases such as Petrobras, Tenet Healthcare, VW, and BP's Deepwater Horizon monitorships.

Chen received her B.A. from the University of California at Berkeley and her J.D. from the University of California in Los Angeles. She is a member of the District of Columbia Bar.

She authored the Fraud Section's "Evaluation of Corporate Compliance," and consulted on all Fraud Section corporate monitorships, including hosting a training for monitors on best practices and lessons learned.

Prior to her retainer with the DOJ, Chen served as a senior compliance leader in such industries as: technology, pharmaceutical, and financial services. In these roles, she worked closely with business leaders to design and implement compliance programs, conduct risk assessments, supervise global internal investigations, and enhance compliance financial processes and controls.

MITRATECH

WWW.MITRATECH.COM

About Jason Cropper

Having over ten years of experience in the software industry, Jason Cropper came to Mitratech through acquisition of Hitec Laboratories in August 2016. As Vice President of Business Development - GRC, his focus within Mitratech is to help clients with their governance, risk, and compliance requirements.

About Mitratech

Mitratech is a market-leading provider of legal, compliance and operational risk solutions for more than 1,200 organizations of all sizes across the globe, representing almost 40 percent of the Fortune 500 and over 500,000 users in over 160 countries. Mitratech's portfolio of enterprise legal and risk management software includes legal matter management, spend management, e-billing, legal hold, contracts management, risk management, policy management, audit management and health & safety management.

To learn more, visit www.mitratech.com.

GET IN TOUCH

info@mitratech.com

MITRATECH (US)
+1 (512) 382-7322

MITRATECH (UK)
+44 (0)1628 600 900

MITRATECH (AUS)
+61 (0)3 9521 7077