Cuneyt Akay (00:15):

[inaudible] welcome to the GT ABC podcast. I'm your host Cuneyt Akay. The GT stands for Greenberg Traurig and the ABC stands for anti-bribery and corruption. In this episode, we're going to turn our attention to risk assessments specifically, we're going to discuss the value of risk assessments and where they fit within a broader compliance program. What the us government expects from companies in terms of risk assessments, and finally discuss some suggestions for how to conduct and utilize the information gained from these risk assessments. My guest on this episode is Tyler Coombe, who is a shareholder in GTS Denver office for the last decade. Tyler has focused his practice on anti-corruption compliance and investigations, supporting clients in all aspects of FCPA and UK bribery act compliance. Tyler has conducted anti-corruption risk assessments for companies engaged in various businesses in countries all over the world, including China, India, Mexico, Brazil, Argentina, Chile, Japan, and the UK among others.

Cuneyt Akay (01:19):

His risk assessment work has landed him in some unusual places, including big box retail stores in South Africa, a shipping terminal in Istanbul and textile factories in Bangladesh. Now on a personal note, despite having an office only a few feet apart in Denver several years ago, Tyler and I both realized that we'd actually seen each other more that year in places like the UK, China, and Mexico. And we hadn't done Tyler, welcome to the podcast. And I'll start with, where do you see risk assessments fitting into a broader compliance program? And what is the general value of risk assessments?

Tyler Coombe (01:54):

Well, first of all, Cuneyt, thanks for the introduction. And thanks for having me on the episode, we have indeed had some interesting experiences around the world, and I'm excited to talk about the topic of risk assessments today. So let's get into it, uh, on, on the role, as you asked the role and value of risk assessments, risk assessments are one of the more fundamental elements of any effective compliance program. It is truly one of the most important functions of the program for several reasons. First, uh, lawyers and professionals in this space are usually versed to some degree in the fundamentals of the FCPA and have familiarity with available guidance. That's out there like for instance, the guidance that DOJ and sec have put out, but it can be tricky to put those concepts into action and actually craft a compliance program that works for a company, a program that addresses the company's specific risks and allocates resources to the higher risk areas.

Tyler Coombe (02:53):

Risk assessment is a key part of establishing the risk profile of the business so that you can then form a foundation for the program, tailor your compliance measures and resources to the contours of that business. Uh, another critical piece of, uh, of risk assessments. They're not only important to do at the outset. Uh, when you're first setting out to develop design and implement a program, it's very important for the risk assessment to be an ongoing function of the compliance program to be revisited regularly and periodically companies grow and change. For instance, you enter new markets. There may be a new joint venture formed there's turnover in leadership roles and other kinds of changes, uh, take COVID-19, uh, as a great example of this, the pandemic, as we all know, as has quickly caused significant disruption to economies and industries around the world, creating even more urgency to staying on top of how a business is changing and how new risks might be coming into play.

Tyler Coombe (03:54):

So the compliance framework needs to be organic as well to adapt and change along with the business. If you don't run a risk assessment periodically and regularly, uh, like say every year or every couple of years, at least you wind up possibly underestimating or misunderstanding the level of risk and how to address it or even worse, you might completely miss things and fail to allocate resources or install mitigation measures. And one other thing I'll say Cuneyt about, uh, the, the role and importance of risk assessment. It's, it's just a healthy exercise for a business to go through periodically. It fosters connections between people, uh, whether it's compliance professionals, members of the legal team, business leadership and people in functional roles. It's really an opportunity to dig in, to learn what a company is doing day to day on the ground, nuts and bolts, you know, both at a high level and down in the weeds, we learn a lot about the company, its challenges and successes evolution of the business, et cetera.

Tyler Coombe (04:57):

And we also connect as people and colleagues. There's a lot of value in that. It not only serves the more immediate risk of your, your risk assessment goals, but it helps all of the segments of the business get on the same page, have a better understanding of what each other is doing. Uh, and that helps the compliance function of a business even more to be more effective and, and really hopefully to be viewed as more of a partner and a resource to the business rather than a burden or an obstacle as sometimes, unfortunately is the case. So having said that, Cuneyt, um, and we know that a risk assessment is a fundamental component of a compliance program, but where does this come from? Uh, what is expected of a company to do

Cuneyt Akay (05:38):

Well, Tyler, as you mentioned, you're right. I mean, risk assessments are fundamental to developing a strong compliance program and that has been highlighted by the DOJ and the sec in both additions of the FCPA resource guide and also by the DOJ and the evaluation of corporate compliance programs, guidance in both the resource guide and evaluation of corporate compliance programs, guidance. Both of those were updated earlier this year. In fact, over the spring and summer, and from we see there is that risk assessments help inform companies on how to design their compliance programs. And this is important because a compliance program should be tailored to the company's specific risks as a DOJ and sec have stated in the FCPA resource guide, a one size fits all compliance program is generally ill, conceived and ineffective because resources are spread too thin with too much focus on low risk markets and low risk transactions, which of course come to be a detriment to the company in terms of focusing on higher risk areas and higher risk of transactions.

Cuneyt Akay (06:39):

For example, I recently advised a company that had a robust hospitality policy and then recently invested in a system to track and approved meals and entertainment. Well, there are a couple of issues. One was, uh, one issue was that the company didn't entertain all that much, what the company did often was provide gifts, which weren't tracked in this system that they invested in. And the company also had little to no visibility into their discounts and concessions, particularly to government entities and government officials, which as we found out later posed a larger risk to the company because of the frequency and the value of those discounts and concessions. Now, the DOJ recently focused a lot of attention on risk assessments in the evaluation of corporate compliance program guidance, which provides a lot of useful insight into what is expected of companies by the U .S. Government.

Cuneyt Akay (07:32):

And in this guidance, there's three fundamental compliance questions that are asked. And the first question is whether a company's compliance program is well designed. And the first factor the DOJ discusses in the design of a compliance program is risk assessment. And in this guidance, the DOJ has stated that prosecutors can consider whether companies analyze and address the varying risks presented by numerous factors, including the location of operations, the industry sector, the competitiveness of the market, the regulatory landscape for the company, the potential clients and business partners, the company has. They also look at transactions with government officials and foreign governments payments to foreign officials. They look at the use of third parties, gifts, travel, and entertainment expenses, and finally charitable and political donations. So as we'll talk about a little bit later in terms of how to conduct a risk assessment, the us government certainly is laid out in the guidance, the expectations, uh, for companies when they're conducting risk assessments, in terms of what areas they should be looking into.

Cuneyt Akay (08:40):

Now, the DOJ analyzes four things specifically when addressing risk assessments. First is the risk management process. In other words, what methodology has the company used to identify risk and what information or metrics has the company collected to help detect misconduct? The second piece is resource allocation. How does a company allocate resources to ensure it's devoting more time, effort and scrutiny to the higher risk transactions? The third component is evolution and updates. In other words, is the risk assessment current. And is it subject to periodic review? And is that periodic review limited to just a snapshot in time or as we've briefly touched on earlier, is it based on continuous access to operational data? In other words, is it ongoing? And finally, what are the lessons learned? Does the company have a process for tracking and incorporating periodic risk assessment, data and lessons learned from prior misconduct or prior issues into the broader compliance program? In fact, prosecutors may even credit the quality and effectiveness of a risk-based program that votes appropriate attention and resources, the high risk transactions, even if it fails to prevent an infraction that's coming directly from the DOJ guidance. Now, Tyler, you know, one of the questions that comes up is how to conduct a risk assessment. And what are some of the newer ways or tools to help conduct a risk assessment, especially when people are working remotely and not traveling as much

Tyler Coombe (10:17):

Well, Cuneyt that's, uh, viewed by many as the million dollar question. Uh, you know, though there is guidance and there are principles articulated that as you just went through the how part is, is left largely for us to figure out as it should be. You know, as you mentioned, there really can't be a one size fits all approach and, and there isn't an off the shelf option for running a risk assessment. So the challenge really is to translate those concepts of risk assessment against the backdrop of the guidance that you, that you went through and formulate an approach that makes sense for your business. And this can be somewhat daunting, especially nowadays during a COVID-19 pandemic, which has disrupted, uh, many aspects of business, uh, not the least of which is, is connecting with people, um, and, and having access to information, um, within a business.

Tyler Coombe (11:09):

But there are some key components that should be included in, in any risk assessment process. And, and this can serve as a starting point for outlining what your risk assessment will look like. Number one, establish a scope and methodology for the risk assessment. And we'll get into more detail for each of

these in just a moment. Uh, and that's number one, number two, conduct, uh, an information gathering process, uh, that will garner the right information. Uh, and here's where some technology will come into play because especially during these times, um, access to information can be challenging. There are technologies available, uh, to help us connect with people and gather information, number three, then analyze the results of your work, uh, the information gathered, uh, and then formulate actions response to that information that you've gathered that addressed the risks that you've identified. Uh, and that, that process, that, that is the cycle that we need to follow, uh, to really run a thorough risk assessment.

Tyler Coombe (12:14):

So let's talk about those in a little bit more detail, as I said, the first, first piece of this is defining a scope and a methodology that you'll find at the outset think, think big, what's the big picture? What, what parts of the business will be in scope? What will will be your work plan to collect information and then analyze it? Uh, so in terms of scope, is it enterprise wide side or is it focused on a particular business division or perhaps a particular geographic region pin down the scope of review and then outline a methodology to be used to gather the right information for analysis within that that's scope, uh, often the most model or the method use to organize the information in order to kind of conceive of your methodology is to define the subject matters that you'll be focused on that is what are the kinds of business activities that may involve higher risk transactions, where there's likely to be some, some kind of contact or interaction with a foreign government official, especially if you're you're FCPA focused, you know, some examples would be, and you went through some of them Cuneyt in talking about the, the DOJ guidance, where is the business going to have interactions that you'll want to hear more about, uh, where there is, uh, um, the business is making a, uh, making a play to win, uh, a government contract, for example, or in relation to business development, there is the giving of gifts and entertainment.

Tyler Coombe (13:45):

If the business needs to obtain, or in some circumstances, renew, uh, certain kinds of licenses or permits, these are the kinds of things that you'll want to include within your, your work plan, the kinds of subject matter areas that you'll need to drill into then within each of those subjects, it's an opportunity really, to, in the course of gathering information, find out the specifics of what the business is doing and who's doing it. And, uh, is it directly, or are there third parties involved? This will put you into the information gathering phase, but what you're doing is setting up a structure to capture the information, to, to describe the nature and frequency of activities. So you'll be able to conduct the analysis down the road to factor in things like the likelihood, uh, that, that some improper action may be taken or that a solicitation could occur and to weigh the possible negative impacts if such a, an improper action does occur.

Tyler Coombe (14:37):

And then of course, to be considered to, to include some, some gathering of information, some analysis of whether the company has risk mitigating measures in place that that would reduce that risk, uh, like internal controls or certain procedures or systems technologies in place that, that might address those risks. And then ultimately you have at the end through that process, that analytical model, you'll, you'll have some picture of the nature and degree of any remaining or, or residual risk that that is they're utilizing this framework. The idea is to define the scope, outline a work plan, uh, identify the source of that information. So it's, it's good to have the, the analytical framework of course, and, and how to gather information, but a key part of the plan to do so is identifying the sources of those information, whether that's certain key personnel documents, perhaps pulling some data from different sources and

have a really clear plan that provides a structure, a timeline that you'll follow. And that will facilitate communicating with people in the business, communicating with leadership, people know their roles and responsibilities what's expected from them. So you can run a risk assessment according to plan a in an orderly way to accomplish what you need within the timeframe you have.

Cuneyt Akay (15:53):

And the point about scope. Are you suggesting that risk assessments only focused on anti-corruption or could the scope of the risks assessment there'll be on that?

Tyler Coombe (16:01):

Yeah, that's a great question. More and more frequently now companies are choosing to include anti-corruption as one subject within a broader compliance risk assessment, uh, that, that might cover a whole array of different compliance areas or topics. And that's, that's good. That can be really effective and actually very cost-effective to include an anti-corruption as, as one part of a broader assessment process. And actually based on my experience that there, there can be some real value in doing that, because if, if anti-corruption is a piece of, uh, of a broader effort and more topics and more issues and scenarios are being discussed, you might pick up on some potential anti-corruption risks that might not otherwise have been identified. Uh, for example, let's say you're, you know, you know, the team or the person is reviewing, um, health and safety issues. Well, you might learn about an instance of non-compliance in, in some facility in some country, maybe there was a violation or citation of some of some sort by local health officials, which resulted in the company having, having to go resolve that.

Tyler Coombe (17:07):

And there was a previously unknown government contact in relation to resolving that citation. Well, you know, flags go up, if you're kind of listening from an anti-corruption perspective, you'll pick up on that. And, and you'll, you'll be able to factor that into the ACPC, even though there may be some other health and safety or other compliance issues identified there as well. So if anti-corruption is combined, uh, it, it can certainly have some value. I would caution that or suggest that if that does happen, it is important for anti-corruption still to have a defined role within that process. And that for someone with anti-corruption specific experience, be involved in that because anti-corruption can be fairly nuanced, not always so straightforward to identify where there's some potential risk. So involve somebody who knows, who knows how to pick up on those things as well. With that, let's now get into the process, uh, of, of information gathering a little bit more in depth.

Tyler Coombe (18:03):

Uh, and I think an important thing to remember here is that the quality of the information you obtain is critical. You know, you've, you've outlined a methodology and a scope, and you get into the process of maybe meeting with people, uh, pulling information. Uh, but if you get unreliable or incomplete information in that process, then your results of your risk assessment, likewise, may well be unreliable. Uh, so the focus should be on getting good information. And what are the, what are the methods that we typically employ to, uh, obtain information and as part of the risk assessment process often, and, and extremely valuable is doing in-person interviews or meetings with people, uh, with certain roles and responsibilities to connect with people using a web conferencing platform like zoom document gathering from various business segments, data mining, and analytics of the data is one potentially very valuable area.

Tyler Coombe (18:58):

And then also looking at past risk assessments, the reports from those, and perhaps other internal reviews. And I want to say a few words about interviews. It, it remains one of the best methods really to connect with the business and find out what's going on. I think most of us who, uh, work in this area understand that it's very valuable to meet face to face. And it's sometimes a bit of a luxury to be able to get face to face with people, especially times like now, but it's worth a reminder of that. Having the eye contact and seeing body language in meetings is extremely valuable. And I just want to point out an example, this has happened several times when I've been able to be on site to assist in a risk assessment. Well, you know, there are times when you have a scheduled meeting or interview, you have an agenda, you follow it.

Tyler Coombe (19:46):

Maybe you have some prescribed questions that you, and that you include in that process and you wrap it up and, and, uh, people move on. Whereas if you're on a, on a, on a zoom call or, or even a phone call that that might be the end of the, the conversation when you're on the ground, there are, there are other opportunities. You continue to talk to people. You may be walking down the hall, uh, and, and meet somebody you didn't talk to before, or continue a conversation that started earlier in the day. Perhaps you go out to lunch with somebody or, or dinner. Uh, you hear things that may not have been raised during other, you know, the, the earlier meeting, uh, or may not have been articulated in quite the same way. This happens, uh, all the time. And it really gives you a richer and more round understanding of the issues that you've been targeting.

Tyler Coombe (20:32):

And there's just this kind of ancillary value and benefit to doing it. So it's great if you can do it, but especially now, as we've already mentioned, given the COVID-19 pandemic, we're all living through tough times and, and much more difficult to connect with people and, and certainly fewer opportunities to travel, uh, and to get face-to-face with people, especially if you work in North or with a business that has a far-flung locations. So what do we do about that? What, what options do we have to still run the risk assessment, but, and still get connected to people when, when it's so much harder to do well, our, as already mentioned, we've got platforms like zoom and, and blue jeans, and some of the others that, uh, you know, are getting better and better at connecting us and are more reliable. And you still get some of the face-to-face maybe not as good, uh, with the, you know, as good as, as being on the ground.

Tyler Coombe (21:28):

But you know, that that's, that's the world we live in. And if we have access to those technologies, definitely use them, use them as much as you can chase after people get those meetings set up and do try to connect. So you can see each other and have a more real conversation. In addition to that, though, there are a lot of technology is coming onto the market now, uh, that can apply analytics to data that you pull that can employ, uh, AI functionality in some instances. And it's great if you have access to some of these, you know, internally at your company, absolutely go for it and use it, but, but there are others out on the market too, uh, and, and go seek it out to you. And you'll be amazed at what's available. And one example of that actually, and Cuneyt and I have tried to convert some of our experiences and, and create some technology that provides some, some support, uh, especially at times like this, to really effectively run a, run, a risk assessment, gather information, uh, in an effective,

streamlined, efficient way, provide a framework for analyzing it, give good structure, uh, and, and truly cost saving functionality, uh, uh, to, to those who are running a risk assessment.

Tyler Coombe (22:47):

Um, so that's something we're working on as available. And I encourage everybody really to seek out how technology can, can bolster and support the risk assessment process. It, it remains paramount that we connect with people and get the best information and technology really can help in that respect.

Cuneyt Akay (23:02):

Well, teller is a huge describing all these efforts to gather information, whether that's in person meetings with personnel, you know, visiting company sites, or looking at different types of data, what can you say? And what can you tell us about where this information should go? And maybe more importantly, what should companies do once they've collected and gathered this data?

Tyler Coombe (23:23):

Excellent point Cuneyt, and really that's, that's the crux of the process. And you mentioned earlier, this, this is one of the criteria included in the DOJ guidance, uh, that you have to use the results of the risk assessment. And, and I like to look at this as a cycle, uh, and it's really important to complete the cycle. So you can look at this as is the final phase. You've, you've established a scope and methodology and run through different forms of, of information gathering, but then what do you do with it? It's one of the main challenges that, that a lawyer or a compliance professional will face how to weigh and evaluate that information to exercise judgment, to make determinations about how much risk the company faces in certain areas. It's interesting. The process in my experience is as much art as it is science. There, there isn't a prescriptive model, uh, or any standard or formula.

Tyler Coombe (24:21):

And often there's really no clear answer. You just have all of this information and have to make heads or tails of it. What I like to encourage people to do is use your experiences and take advantage of the resources that are available to you. And one way to do that, um, this kind of goes back to the, the methodology that we were talking about a minute ago, but you have an analytical framework. If you've, if you've set it up to identify the subject areas and you delve into the details of different kinds of business activities and transactions, and you've captured that information well, get into the details of each of those things. What have you learned about those, those, the transactions and activities that, that may have some anti-corruption implications? What are the consequences that potentially come from those activities? And what's the likelihood that those could occur.

Tyler Coombe (25:14):

You should evaluate for each of these issues. And you could think of them kind of as line items of, of issues you've spotted in the course of, of, uh, gathering information, but evaluate then if they're, if they present some risk, to what extent are there mitigating measures in place, uh, that will reduce the risk or, or, uh, affect it somehow. And then finally at the end of that, there's, for many of these will be some amount of residual risk, and that's really what we're trying to get to what, what remains that, that requires the attention and the devotion of resources to address, uh, you you've gotten to this end point and it's, you know, I I've seen this done different ways at times. Uh, you can sort of apply a scoring method that you, you rate the, the risk presented by a particular kind of activity, and it gets a certain score, and that might be reduced by certain mitigating measures you've identified.

Tyler Coombe (26:08):

And maybe there's a resulting score that, that you can plot on some, on some scale. That's fine. Um, don't have to do it that way. That is one way though, to kind of organize the, uh, the information and rank it, some like to do heat maps and assigned colors and things like that. And that's fine too, at the end of the day, what we need to get to is those things that should be considered high risk, or can be, uh, thought of as medium or low risk. This is all about. And this goes to the DOJ guidance, allocating resources to where they need to go, where are the higher risks? So this analytical process should, you know, everything flows and funnels through it. At the end of that, the desired outcome is, um, pay a reasonable determination of what are the higher risks. And from there, this is really the, the closing of the loop as outlining actions that the business should take to address those specific risks.

Tyler Coombe (27:04):

Sometimes it's called the feedback loop, or that there are action plans developed, but that really is important. This is the piece that is you can't allow the business after a risk assessment to, in a sense, become pregnant with the information about its risks, make a plan for reasonable and proportionate action to address those risks. You know, for an example, if the, you may learn for the first time that a business unit, uh, is looking to invest in a special economic zone, say in Southeast Asia, well, who's going to be involved. Have they been trained? Are there going to be third parties involved to help get government permissions, these kinds of things. And you will have gathered some information around that, but if some of those things aren't happening need to happen, that's the basis of an action plan to, to say, let's do these steps that will address this new thing that the business is going to do, and then follow through on that. And then, you know, the, the cycle will continue the next time around, perhaps it's the next, uh, risk assessment next year. You'll come back to that and, and look at what you identified then what was the plan? Did you do it and what has changed or what's new about that particular circumstance?

Cuneyt Akay (28:15):

Well, Tyler, thank you for walking us through some suggestions in terms of how to conduct a risk assessment and what to do with the information that you've gathered once you've conducted that risk assessment. And thank you for joining us on this episode of the GT ABC podcast. Tyler, I think there's really three main takeaways I have on this topic regarding risk assessments. First is risk assessments are fundamental in a core component of developing a strong anti-corruption compliance program. Second, the U.S. Government has made it clear that simply conducting a risk assessment. Isn't sufficient companies should have a methodology for identifying risk. They need to have continuous access to operational data companies should allocate resources to higher risk transactions and higher risk areas. And they should incorporate the lessons learned from those risk assessments and from prior misconduct into their own compliance programs. And finally, an effective risk assessment should have a thoughtful scope and methodology and a good work plan to gather information whether in person or through the various technological tools that Taylor referenced earlier, and then evaluate the results of that risk assessment to help mitigate the company's risk and to help strengthen the company's platform.

Cuneyt Akay (29:30):

Thank you for tuning in and listening to this episode of the GT ABC podcast.

Tyler Coombe (29:41):

[inaudible].