

# OPEN AIR BLOG

## Case Study #5: Even a Stopped Clock

You probably think by now that I'm a crusty, irascible curmudgeon. I've had absolutely nothing positive to say about these case studies. All this negativity is getting me down, and me, such a lovely fellow (or so say my kids).

It delights me to tell you that if you're a small company looking to do a risk assessment on the cheap, case study #5 is a must-read. I've also realized that in discussing these case studies, I've been neglecting to include commentary on the Principles that underlie the UK government's suggested remediating points. A glaring omission that I realized while soaking up the great posts of my colleague Tom Fox (an everyday read for me). What I'm happy to report is that Principle 3, on risk assessments—while far from perfect—is really very good.

I've been “in the middle of” drafting a mammoth post on risk assessments for about 3 weeks now. I'm feeling inertia set in on that post, so I'll include some of my suggestions from that post in here.

What's important to remember is that most companies—I'm tempted to say “all companies,” but I like to leave room for my own incomplete knowledge—have a risk assessment that, in a word, sucks. There are exceptions, I'm sure, but most aren't as rigorous as their creators think they are, or don't cover the right things, or are back-of-the-napkin, or are anecdotal. I've seen far too many compliance officers skip this important step, rationalizing that they have a good handle, from their gut, on the risks the business face.

Here's something that you don't hear often, but it's a true statement that you ignore at your peril: you need two risk assessments. Risk assessment #1 is where corruption falls on your enterprise risk chart. This pits corruption against other risks like money laundering, sanctions/export, antitrust/fair competition, privacy, and other regulatory risks specific to your business. Some companies combine all these into one “regulatory risk” category and four-box it along with operational risks. That's one way to go. Reasonable people can disagree which model is better, and it comes down to your specific business model. My preference is the former, but people smarter than me choose the latter also. The reason you need this cross-risk assessment is to justify where you're spending—and more importantly, not spending—your limited budget. If your diligence is lacking on a third party, it's hugely beneficial to be able to show that you weren't ignoring that risk, but your budget this year went to another risk mitigation effort.

Your second assessment is particular to corruption, and helps you determine where your anti-corruption budget should be spent this year. The most important two words in that sentence are the last two. A risk assessment lasts a maximum of one year. Often less, because the business

changes fast. If the business reorganizes, your risk profile changes. If your business introduces a new product or enters a new market, your risk profile changes. Spend an hour and update your assessment: talk about great optics!

Before I get to what the right process is for a risk assessment, let's look at the case study, and what the MOJ's suggestions are.

Case study #5 posits a small specialist manufacturer who wants to expand into a new market, but hasn't decided which market. The firm has no particular risk-assessment expertise, and is a little lost.

The MOJ's optional suggestions are:

- Incorporate bribery risk into the business' market analysis (presumably alongside customer base, competition market share, ease of entry, labor costs etc.)
- Seek advice from UK government sources like embassies and Chambers of Commerce
- Consult the TI list (it says "general country assessments undertaken by local chambers of commerce, relevant non-governmental organizations and sectoral organizations," but it means the TI list)
- Seeking advice from industry reps, and
- Follow up with independent research

Here's where I'm happy to say that I really like this list. Excellent job, MOJ! Except for the one about seeking advice from industry reps. What were you thinking on that one? This is an extremely sensitive and strategic decision: the idea that you'd ask outsiders for advice, absent an NDA or fiduciary relationship is ludicrous. But other than that, well done!

Let's talk about this for a second. First, the hypothetical posits a small company. For larger companies, for Heaven's sake, call Manny Alas at PriceWaterhouseCoopers and get some professional advice. Tell him I sent you and he'll give you a free set of steak knives. (kidding). I doubt anyone better at this than Manny exists on the planet, but if you have someone else, the point here is to pay the money and get the advice you need.

Smaller companies can't afford that level of completeness, and have to compensate. I love, absolutely love, that first suggestion. So much so, in fact, that I'd recommend it for every company of any size. It's hard to overstate how important it is that you embed compliance discussions in business discussions. Not just for anti-corruption, for everything. I have this mantra: there's no such thing as "compliance training," it's all business training. A person can't do their job well if they don't meet their targets, and can't do their job well if they embroil the company in a regulatory issue. I'd broaden that statement to include all of compliance: all controls are business controls. The more integrated your compliance program is with your business processes, the better off you are. A great start is with someone as basic as market choice. Why wouldn't the business equate corruption costs with labor costs in their thinking?

Point 2: seeking advice from government sources. Absolutely. It's free, looks great, and doesn't take much effort. A trifecta! My addition here is to consult the embassies of each market you're considering. They'll have the on-the-ground experience that will prove invaluable. I used to poo-poo embassy calls. But the panel on Africa at the Global Compliance Symposium changed my mind. If Billy Jacobson, Sophie Lamont, and Herbert Ignobogu—the three who I was so impressed with—say it's a good idea, who am I to argue?

Point 3: consult the TI list. There are other lists out there, but Transparency International's Corruption Perceptions Index (aka "the TI list") is the authoritative one for corruption. Everyone uses it, companies, regulators, everyone. Looking at other lists lends a great coat of polish to an inexpensive risk assessment, but the TI list is mandatory. I've never worked at an extractive industry corporation, or pharma company, so there might be industry-specific lists out there of which I'm unaware in those, or other, industries. For financial services, there are money-laundering country lists out there. In any event, those will be in addition to, not instead of, the TI list.

Point 4: industry reps. As I said, this is unrealistic, if not downright silly. But if you don't care if your competition knows your strategic plans, go to town.

Point 5: following up with independent research. Maybe a little flavor here of the water-is-wet obviousness that I've painted other case studies with. But I'm always amazed at the ridiculously obvious things some companies don't do, so I'll reserve that particular complaint and say that any amount of follow-up research is like gold. A little is great, more is better. But it's always true that a little is better than none. And with the Internet, research is easier than ever. Here's one example of market diligence gold. If you're looking at a risky market, use the Internet to find the name of a dissident in exile, and arrange a phone interview; ask that person what the risks are of doing business in that market. Incorporate at least one suggestion from that conversation into your program. Can you imagine how diligent that makes you look? If you can't arrange a conversation, find newspaper articles about the dissident, in which I'm sure you'll find some tidbits about the risks of having a presence there. I'm ready to give you an NPA right now.

Another suggestion: ask TRACE. If you don't know about TRACE, it's a member organization with great resources. It costs a little money, but it gives great value for the money. And not for nothin', but I put my money where my mouth is on this: I had both companies I worked for join, or renew, membership. Call Alexandra Wrage (the last name rhymes with "foggy," you'll be a step ahead if you pronounce her name right); I'm a fan, and it'll be worth it.

Let's turn now to the Principles. The first point made in Principle 3 is that the risk assessment should be periodic, informed, and documented. I can't think of anything to add to that statement. The commentary to the principle recognizes first that the risk assessment will be part of an overall business effort to examine business risks. Dead on. The MOJ suggests that the assessment process requires a) top-level oversight, b) appropriate resourcing, c) identification of information sources, d) diligence inquiries, and e) documentation. Exactly right. I personally think the information

sources issue will probably be the hardest, but in practice, the resource allocation issue probably takes first place. You can get by with a “quick and dirty” assessment for a while, but you’re going to need a real one sooner or later.

The commentary on principle 3 also recognizes that risks change over time, and therefore so will the risk assessment. It’s a living document, in other words, and should be re-evaluated often.

Here’s where the commentary really gets good. It lists five commonly encountered risks:

- Country
- Sectoral
- Transaction
- “Business Opportunity” risk
- Business Partnership

We’ve talked already about the first two, so let’s skip to the third. My reaction: YES!! Transaction risk is too often ignored. This is doubly true with third-party diligence, where a third party gets cleared to form the relationship, and the diligence stops. Once you bring a high-risk third party on board, you need to monitor the transactions to ensure that riskier transactions get their own response.

I think that “business opportunity risk” is just another flavor of transaction risk, at least from how it’s written up in the commentary to principle 3.

Transaction risk first and foremost identifies and analyzes the financial aspects of the deal. Is there money left on the table, or money that’s spent in a non-transparent way? Who is the end-user?

The commentary then moves onto internal risks, and again does a fantastic job:

- Where is your training lacking?
- Do you have a culture that rewards excessive risk-taking?
- Are your policies prohibiting bribery unclear? (Or, I’d add, are they written by lawyers and for lawyers)
- Are your financial controls unclear?
- Is there a lack of effective messaging from the top?

This is an excellent list. The only thing I’d add is to point two: in addition to asking whether the culture celebrates risk, I’d ask how your salespeople are measured. If only on the amount of sales, I’d take that into account. I would also pay special attention to your financial controls. You need to identify what financial controls you have and link-and-label them back to your anti-corruption program. When you say, here’s my anti corruption program, your total gamut of financial controls needs to be identified.

Now we've reached an inflection point, and I'll give you another true statement you ignore at your peril: a risk assessment is a tool, a compass, not an end unto itself. I really like the word "compass" here. A risk assessment points your compliance program in the right direction.

You take your risk assessment and structure your resources, both time and money. If you find that your training is deficient, you need to prioritize that in your spending. Are your procedures tailored to your riskiest employee base? Do you even know who your riskiest employees are? Can you say with assurance that your financial controls will keep someone from signing an invoice to pay for \$100,000 worth of services that were never provided? Your risk assessment should tell you these things.

And how do you get to this nirvana? What's the process you should follow? Well, the most common answer would be "surveys." That's not entirely correct, and it's not something that the guidance tells you. The most important thing about conducting a thorough risk assessment is involving the right people. You need a group at all levels of the organization; the more the merrier. You need the entire leadership team, and you need legal and compliance. You need to understand what's actually going on in the organization, because that's where you'll capture real risk, rather than theoretical risk.

In any case, for smaller companies, this case study is great. I'm tempted to say that even a stopped clock is right...twice every day. But let's celebrate the good job that they did here.