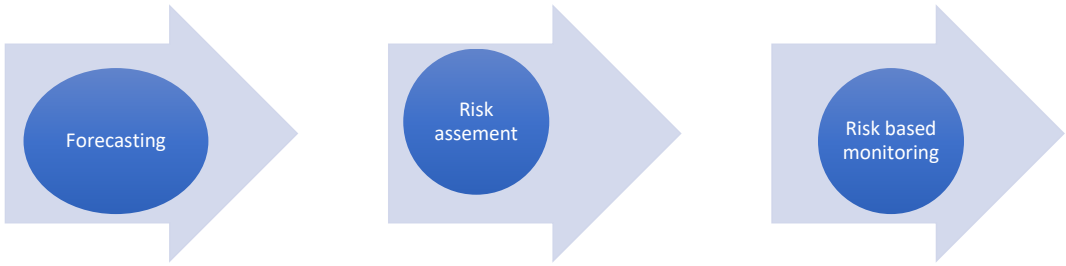
Thomas Fox

The Compliance Evangelist

A. Measuring your risk

Operationalizing your compliance program can take many shapes and forms. Using the entire risk management process to embed your compliance program within the contours of your organization is an important, key step as it will allow you to have full visibility of your compliance risks through a longer life cycle. Forecasting allows you to consider your business strategy and wed the risks you can foresee. Risk assessments allow you to evaluate and measure known risks. Risk-based monitoring allows you to monitor both the compliance risks you know about and detect those you do not know, on an ongoing basis.

I think there are several key lessons to be considered by any Chief Compliance Officer (CCO) or compliance practitioner. The first is the process around risk management. Most compliance practitioners understand the need for a risk assessment as it is articulated as Hallmark No. 4 of the Ten Hallmarks of an Effective Compliance Program. From the 2012 FCPA Guidance, the DOJ and Securities and Exchange Commission (SEC) said, "Assessment of risk is fundamental to developing a strong compliance program, and is another factor DOJ and SEC evaluate when assessing a company's compliance program." In addition to this business case, the 2012 FCPA Guidance also specified the enforcement reasons for performing a risk assessment, "DOJ and SEC will give meaningful credit to a company that implements in good faith a comprehensive, risk-based compliance program, even if that program does not prevent an infraction in a low risk area because greater attention and resources had been devoted to a higher risk area." The DOJ Evaluation of Corporate Compliance Programs builds on this.



Yet as compliance evolves, and corporate compliance programs become more sophisticated, compliance is seen not as simply a legal prophylactic, but as a business process. Seen in this light, it is clear the risk management process should begin with forecasting as it attempts to estimate future aspects of your business. Compliance professionals should be able to say with some degree of authority, what will happen in the next three months, six months, twelve months, twenty-four months. This can facilitate resources deployment where they think is appropriate in order to meet these future demands.

By starting with forecasting, a compliance function utilizes risk assessment to consider issues which forecasting did not predict for or issues which the forecasting model raised as a potential outcome which warranted a deeper dive. If you are moving into a new product or sales area and

are required to use third-party sales agents, a risk assessment would provide information that a company could use to ameliorate the risks. Risk-based monitoring follows on from the issues that your risk assessment identified as your highest risks. Risk-based monitoring tends to look at things on an ongoing basis, and the models that are behind the risk-based modeling, are continuously refined based on incoming data.

All of these three tools tie back into process management and process improvement. There is a balance between what is actually important for your business or for proper execution; versus the practical aspects of the whole process. Ben Locwin stated, "If you are not measuring at a high enough resolution, then you are not capturing a lot of the environmental, market forces and external factors that probably are of high leverage to your operations in business that you simply do not know about."

For example, if there is a one-in-three chance of a compliance failure occurring, which a company knew that in advance; the executive committee probably almost stop the activity before there was a compliance failure and possible legal violation. This is how the risk management process can work to fulfill the three prongs of a compliance program, *prevent, detect and remediate.* You are using your risk forecast and you have a contingency in place, which you execute upon. In other words, it comes down to execution. This means you have to use the risk management tools available to you and when a situation arises, you remediate when required. This is not only where the rubber hits the road but the information and data you garner in the execution phase should be fed back into a process loop. From this, you will develop continuous feedback and continuous improvement.

I have gone through this in some detail to emphasize the business process nature that compliance has evolved into as a corporate discipline. By using these techniques, the CCO or compliance practitioner makes the business run more efficiently and at the end of the day, more profitably. The more you can bring these types of insight to a Chief Executive, the more you demonstrate how compliance adds to the bottom line and is not simply a cost center.

Three Key Takeaways

1. The risk management process is an important backbone of operationalizing compliance.
2. You should be able monitor and measure both known and unknown risks.
3. All of these steps help a business to run more efficiently and more profitably.

B. How to Perform a Risk Assessment

One cannot really say enough about risk assessments in the context of an anti-corruption programs. Since at least 1999, in the *Metcalf & Eddy* enforcement action, the DOJ has said that risk assessment which measure the likelihood and severity of possible FCPA violations the manner in which you should direct your resources to manage these risks. The 2012 FCPA Guidance stated it succinctly when it said, "Assessment of risk is fundamental to developing a strong compliance program, and is another factor DOJ and SEC evaluate when assessing a company's compliance program."

This language was supplemented in the 2017 in both the Evaluation and the new FCPA Corporate Enforcement Policy. Under Prong 4 of the Evaluation, Risk Assessments, the following issues were raised: **Risk Management Process** – *What methodology has the company used to identify, analyze, and address the particular risks it faced?* **Manifested Risks** – *How has the company's risk assessment process accounted for manifested risks?* In the FCPA Corporate Enforcement Policy it stated, "The effectiveness of the company's risk assessment and the manner in which the company's compliance program has been tailored based on that risk assessment".

The risk assessment determines the areas at greatest risk for FCPA violations among all types of international business transactions and operations, the business culture of each country in which these activities occur, and the integrity and reputation of third parties engaged on behalf of the company. The simple reason is straightforward; one cannot define, plan for, or design an effective compliance program to prevent bribery and corruption unless you can measure the risks you face.

Rick Messick laid out the four steps of a risk assessment as follows: "First, all conceivable forms of corruption to which the organization, the activity, the sector, or the project might be exposed is catalogued. Second, an estimate of how likely it is that each of the possible forms of corruption will occur is prepared and third an estimate of the harm that will result if each occurs is developed. The fourth step combines the chances of occurrence with the probability of its impact to produce a list of risks by priority."

What Should You Assess?

In 2011, the DOJ concluded three FCPA enforcement actions which specified factors which a company should review when making a Risk Assessment. The three enforcement actions, involving the companies Alcatel-Lucent, Maxwell Technologies and Tyson Foods all had common areas that the DOJ indicated were compliance risk areas which should be evaluated for a minimum *best practices* compliance program. In both Alcatel-Lucent and Maxwell Technologies, the Deferred Prosecution Agreements listed the seven following areas of risk to be assessed, which are still relevant today.

1. Geography-where does your Company do business.
2. Interaction with types and levels of Governments.
3. Industrial Sector of Operations.
4. Involvement with Joint Ventures.
5. Licenses and Permits in Operations.
6. Degree of Government Oversight.
7. Volume and Importance of Goods and Personnel Going Through Customs and Immigration.

All of these factors were reiterated in the 2012 FCPA Guidance which stated, "Factors to consider, for instance, include risks presented by: the country and industry sector, the business

opportunity, potential business partners, level of involvement with governments, amount of government regulation and oversight, and exposure to customs and immigration in conducting business affairs."

These factors provide guidance into some of the key areas that the DOJ believed can put a company at higher corruption risk. These factors supplement those listed in the now withdrawn UK Bribery Act Consultative Guidance which stated, "Risk Assessment - The commercial organization regularly and comprehensively assesses the nature and extent of the risks relating to bribery to which it is exposed." The UK Bribery Act Consultative Guidance points towards several key risks which should be evaluated in this process. These risk areas include:

1. Internal Risk - this could include deficiencies in
- employee knowledge of a company's business profile and understanding of associated bribery and corruption risks;
- employee training or skills sets; and
- the company's compensation structure or lack of clarity in the policy on gifts, entertaining and travel expenses.

2. Country risk – this type of risk could include:
(a) perceived high levels of corruption as highlighted by corruption league tables published by reputable Non-Governmental Organizations such as Transparency International;
(b) factors such as absence of anti-bribery legislation and implementation and a perceived lack of capacity of the government, media, local business community and civil society to effectively promote transparent procurement and investment policies; and
(c) a culture which does not punish those who seeks bribes or make other extortion attempts.

3. Transaction Risk – this could entail items such as transactions involving charitable or political contributions, the obtaining of licenses and permits, public procurement, high value or projects with many contractors or involvement of intermediaries or agents.

4. Partnership risks – this risk could include those involving foreign business partners located in higher-risk jurisdictions, associations with prominent public office holders, insufficient knowledge or transparency of third party processes and controls.

Another approach was detailed by David Lawler, in his book *"Frequently Asked Questions in Anti-Bribery and Corruption".* He broke the risk areas to evaluate down into the following categories: (1) Company Risk, (2) Country Risk, (3) Sector Risk, (4) Transaction Risk and (5) Business Partnership Risk. He further detailed these categories as follows:

1. Company Risk-Lawyer believes this is "only to be likely to be relevant when assessing a number of different companies – either when managing a portfolio of companies from the perspective of a head office of a conglomerate or private equity house." High risk companies involve, some of the following characteristics:

- Private companies with a close shareholder group;

- Large, diverse and complex groups with a decentralized management structure;
- An autocratic top management;
- A previous history of compliance issues; and/or
- Poor marketplace perception.

2. Country Risk-this area involves countries which have a high reported level or perception of corruption, have failed to enact effective anti-corruption legislation and have a failure to be transparent in procurement and investment policies. Obviously the most recent, annual Transparency International Corruption Perceptions Index can be a good starting point. Other indices you might consider are the Worldwide Governance Indicators and the Global Integrity index.

3. Sector Risk-these involve areas which require a significant amount of government licensing or permitting to do business in a country. It includes the usual suspects of:

- Extractive industries;
- Oil and gas services;
- Large scale infrastructure areas;
- Telecoms;
- Pharmaceutical, medical device and health care;
- Financial services.

4. Transaction Risk-Lawyer says that this risk "first and foremost identifies and analyses the financial aspects of a payment or deal. This means that it is necessary to think about where your money is ending up". Indicia of transaction risk include:

- High reward projects;
- Involve many contractor or other third-party intermediaries; and/or
- Do not appear to have a clear legitimate object.

5. Business Partnership Risk-this prong recognizes that certain manners of doing business present more corruption risk than others. It may include:

- Use of third party representatives in transactions with foreign government officials;
- A number of consortium partners or joint ventures partners; and/or
- Relationships with politically exposed persons (PEPs).

One of the questions that I hear most often is how does one actually perform a risk assessment. Mike Volkov has suggested a couple of different approaches in his article, "*Practical Suggestions for Conducting Risk Assessments*." In it Volkov differentiates between smaller companies which might use some basic tools such as "personal or telephone interviews of key employees; surveys and questionnaires of employees; and review of historical compliance information such as due diligence files for third parties and mergers and acquisitions, as well as internal audits of key offices" from larger companies. Such larger companies may use these basic techniques but may also include a deeper dive into high risk countries or high-risk business areas. If your company's sales model uses third party representatives, you may also wish to visit with those parties or

persons to help evaluate their risks for bribery and corruption would might well be attributed to your company.

There are a number of ways you can slice and dice your basic inquiry. As with almost all FCPA compliance, it is important that your protocol be well thought out. If you use one, some or all of the above as your basic inquiries into your risk analysis, it should be acceptable for your starting point.

Three Key Takeaways

1. Since at least 1999, the DOJ has pointed to the risk assessment as the start of an effective compliance program.
2. The DOJ will now consider both your risk assessment methodology for identifying risks and gathered evidence.
3. You should base your compliance program on your risk assessment.

C. How Do You Evaluate a Risk Assessment?

After you complete your risk assessment, you must then translate into a risk profile, for, as Rick Messick has noted, if the estimate of where bribery is likely occur or its impact if it does occur is wrong, prevention efforts will not be properly targeted. Ben Locwin, explained in "*Quality Risk Assessment and Management Strategies for Biopharmaceutical Companies*", "Once we have assessed risks and determined a process that includes options to resolve and manage those risks whenever appropriate, then we can decide the level of resources with which to prioritize them. There always will be latent risks: those that we understand are there but that we cannot chase forever. But we need to make sure we have classified them correctly. With a good understanding of each of these, we are in a better position to speak about the quality of our businesses."

William Athanas, in an article entitled "*Rethinking FCPA Compliance Strategies in a New Era of Enforcement*" posited that companies assume that FCPA violations follow a "bell-curve distribution, where the majority of employees are responsible for the majority of violations." However, Athanas believed that the distribution pattern more closely follows a "hockey-stick distribution, where a select few…commit virtually all violations." Athanas concludes by noting that is this limited group of employees, or what he terms the "shaft of the hockey-stick" to which a company should devote the majority of its compliance resources. With a proper risk assessment, a company can then focus its compliance efforts such as "intensive training sessions or focused analysis of key financial transactions -- on those individuals with the opportunity and potential inclination to violate the statute." This focus will provide companies the greatest "financial value and practical worth of compliance efforts."

Lawler, suggested that you combine the scores or analysis you obtained from the corruption markers you review; whether it is the DOJ list or those markers under the UK Bribery Act. From there, create a "rudimentary risk-scoring system that ranks the things to review using risk indicators of potential bribery. This ensures that high-risk exposures are done first and/or given more time. As with all populations of this type, there is likely to be a normal or 'bell curve'

distribution of risks around the mean. A 10-15% of exposure falls into the relative low-risk category; the vast majority, 70-80% into the moderate-risk category; and the final 10-15% would be high risk.

In an article entitled, "*Improving Risk Assessments and Audit Operations*" author Tammy Whitehouse focused on how one company, Timken Co. created a risk matrix to evaluate risks determined by the company's risk assessment. Once risks are identified, they are then rated according to their significance and likelihood of occurring, and then plotted on a heat map to determine their priority. The most significant risks with the greatest likelihood of occurring are deemed the priority risks, which become the focus of the audit monitoring plan, she said. A variety of solutions and tools can be used to manage these risks going forward but the key step is to evaluate and rate these risks.

LIKELIHOOD

Likelihood Rating	**Assessment**	**Evaluation Criteria**
1	Almost Certain	High likely, this event is expected to occur
2	Likely	Strong possibility that an event will occur and there is sufficient historical incidence to support it
3	Possible	Event may occur at some point, typically there is a history to support it
4	Unlikely	Not expected but there's a slight possibility that it may occur
5	Rare	Highly unlikely, but may occur in unique circumstances

'Likelihood' factors to consider: The existence of controls, written policies and procedures designed to mitigate risk capable of leadership to recognize and prevent a compliance breakdown; Compliance failures or near misses; Training and awareness programs.

PRIORITY

Priority Rating	**Assessment**	**Evaluation Criteria**
1-2	Severe	Immediate action is required to address the risk, in addition to inclusion in training and education and audit and monitoring plans
3-4	High	Should be proactively monitored and mitigated through inclusion in training and education and audit and monitoring plans
5-7	Significant	
8-14	Moderate	
15-19 20-25	Low Trivial	Risks at this level should be monitored but do not necessarily pose any serious threat to the organization at the present time.

Priority Rating: Product of 'likelihood' and significance ratings reflects the significance of particular risk universe. It is not a measure of compliance effectiveness or to compare efforts, controls or programs against peer groups.

At Timken, the most significant risks with the greatest likelihood of occurring are deemed to be the priority risks. These "Severe" risks become the focus of the audit monitoring plan going forward. A variety of tools can be used to continuously monitoring risk going forward. However, you should not forget the human factor. At Timken, one of the methods used by the compliance group to manage such risk is by providing employees with substantive training to guard against the most significant risks coming to pass and to keep the key messages fresh and top of mind. The company also produces a risk control summary that succinctly documents the nature of the risk and the actions taken to mitigate it.

The key to the Timken approach is the action steps prescribed by their analysis. This is another way of saying that the risk assessment *informs* the compliance program, not vice versa. This is the approach set forth by the DOJ from the 2012 Guidance up to the Evaluation of Corporate Compliance Programs, up to the FCPA Corporate Enforcement Policy. I believe that the DOJ wants to see a reasoned approach with regards to the actions a company takes in the compliance arena. The model set forth by Timken certainly is a reasoned approach and can provide the articulation needed to explain which steps were taken.

Three Key Takeaways

1. Even after you complete your risk assessment, you must evaluate those risks for your company.
2. The DOJ and SEC are looking for a well-reasoned approach on how you evaluate your risk.
3. Create a risk matrix and force rank your risks.