How to Measure Risk Culture Effectiveness: A Practical Guide

Assessing the strength of one's risk management program is no easy task, but organizations that have tone from the top and guidance from middle management can integrate risk awareness and ethics into their DNA, leading to better risk-based decisions.

By Ryan Rodriguez-Wiggins

Establishing a robust risk management framework is critical — but how do we measure the adoption of such a program, and how can we tell if it is actually making an impact? We've already discussed the essential elements and foundation required for building a strong risk management program, and the logical next step is for us to explore the best ways for measuring the effectiveness of risk culture within an organization.

Sadly, there are still organizations that treat risk management as a "check the box" activity. But it's not enough to just have a risk management program in place or a risk team sitting in some far off corner.

Risk management needs to be imbedded in the culture of a firm. It needs to be understood throughout the organization, and must be a topic of daily conversation — rather than something that is only discussed in monthly or quarterly meetings.

Basel's Principles for the Sound Management of Operational Risk defines risk culture as "the combined set of individual and corporate values, attitudes, competencies and behaviour that determine a firm's commitment to and style of operational risk management." It is no coincidence that — of the 11 principles Basel cites — risk culture is at the core of the very first principle: "The board of directors should take the lead in establishing a strong risk management culture. The board of directors and senior management should establish a corporate culture that is guided by strong risk management," the document reads.

While it can be difficult to put a measure on topics like culture, values and attitudes, Basel's operational risk principles give us a good place to start.

Tone from the Top

While it starts with the board of directors (who should influence the C-suite), it is the C-suite and senior management who establish the tone for risk management culture. It is in the goals that they set for middle management; in the messages they deliver down through the firm; and in the topics covered in quarterly town halls. What's more, it is also in what is left unsaid — e.g., do they turn a blind eye to risk if outcomes are desirable?

In one of my former roles, I spent a number of years working for Marcelo Cruz (PhD) — the editor-in-chief of *The Journal of Operational Risk*, an adjunct professor at New York University and author of three books on operational risk. Our team, at the time, knew it was just as important to evaluate gains from errors as it was to analyze losses.

Years ago, this was a difficult concept for traders and profit centers to embrace. They didn't want an "outside" risk group having access to *any* of their errors — let alone their gains or their losses

The profit centers and traders understood that teams calculating operational risk capital use a combination of frequency and severity of loss data in their models. If this loss data is sparse — i.e., if the risk group doesn't have access to trading errors — then capital can potentially be manipulated or lowered.

Of course, without the buy-in of senior management, it would be impossible to track down this data — data necessary not only for modeling but also for root-cause analysis, corrective actions and preventive actions.

It is important to analyze the data for patterns and trends in order to see what area and processes can be improved. A firm that performs this analysis likely has a stronger risk culture than one that just captures the data — or one that doesn't capture this data at all.

Textbook Example: The "London Whale"

The "London Whale" is an example (from 2012) that is particularly relevant to the "tone from the top." This story actually resurfaced in February of 2016, when "London Whale" Bruno Iksil — the trader accused of losing billions of dollars for JP Morgan — wrote a letter.

Breaking a four-year silence, Iksil sent the letter to a number of publications, causing a flurry of follow-up articles to be written. In the letter, he points directly to senior management as the ones who "initiated, approved, mandated and monitored" the trades. In fact, he wrote that his actions in 2012 were not only authorized but that he was "instructed repeatedly by the CIO senior management to execute this trading strategy."

Even before Iskil's letter, it was evident that this amount of losses could not have taken place without a clear lapse in risk management. The letter, however, offers a textbook example of why it is crucial to instill a strong risk management culture from the top.

At this point, it should be clear that while tone from the top is important, it still can be challenging to measure for anyone (including outsiders, external auditors and analysts) who isn't close to the top level of management.

To gain more insight into risk culture at the senior level, here are nine simple questions you can ask:

1. Does the firm have a chief risk officer (CRO)?
2. Does the CRO report directly to the CEO (and/or board) or someone else?
3. Are there mentions of risk management in published firm values, goals or mission statements?
4. Are there established risk committees within the firm?
5. Do the committees have clear and documented charters?
6. How long have the committees been in existence?
7. Is there a dedicated risk management division, group or team?
8. Is there a risk portal or webpage for the risk management team?
9. Do you know who to contact in a risk event?

The Importance of Middle Management

Almost as important as establishing tone from the top is to see that the tone continues down throughout the organization. In the "London Whale" example, senior management had an

important role to play — but, at the end of the day, it is usually middle management and those of us in the front line who make the decision, mistakes and errors that can have a serious impact.

Richard Bistrong, a former international salesperson who got caught up in corruption earlier in his career, offers one strong example of the vital role that middle management can play in a firm's risk culture. As he mentions in the dramatic opening statement on his website, Bistrong "bribed foreign officials," "… cooperated with international law enforcement" and, eventually, went to prison.

Just over a year ago, I was sitting at the GRC Summit 2015 in Washington D.C., listening to Bistrong explain his personal journey — in a very human way — to a room full of a few hundred people. As he described it, back in 2007, Bistrong was working in international sales somewhere near the end of the world at the bottom tip of South America. He was respected, educated and successful at his job.

However, at some point — whether it was because of a lack of oversight, pressure for sales or detachment from a more risk adverse society — Bistrong got involved in facilitation payments.

Eventually, he was caught, and then cooperated with the government for five years in order to bring others to justice and, hopefully, lessen his sentence. Ultimately, Bistrong could not avoid jail time, but his tale is a real, human story with serious impact.

When we hear examples like this, many of us think, "that would never happen to me." But hearing Bistrong speak at the summit offered perspective on how a normal person, in a normal role, can stray from what we would consider normal values.

What could Bistrong's employer have done better to prevent this? It's difficult to say, but perhaps having more frequent compliance training could have led Bistrong down a better path.

Everyday Decisions

It's important for senior management to demand ethics and compliance, but, at the end of the day, it's the decisions that people make in "everyday" roles in the lines of business that drive risk events. There have been countless examples in the news of firms where just one person, or a handful of people, made unethical decisions that had dire consequences.

Just look at any insider trading case, or even the Libor scandal, and the root cause comes down to people. Events can also be the result of sheer mistakes or bad decisions, but more often than not — with the right risk management and controls in place — the damage can be contained or lessened.

While we live and work in a world vastly driven and facilitated by technology, it's still a people business — and those people on the front line have the most exposure. Senior management may err in strategy or objectives, but the majority of risk is managed at the line-of-business level.

Similar to measuring the effectiveness of the tone at the top, it can also be difficult to measure risk awareness and ethics at the team or individual level. But here are some questions that will allow you to "take the pulse" of the broader organization:

- Does your firm tie compensation back to risk management?
- Does your firm include risk management in end of year performance evaluations?
- Does your organization have a whistle-blower program or anonymous complaint tracking system?
- If so, is it actively being used? What types of things are being reported?

- Does your firm have anonymous surveys to gauge employee views on the risk culture of the firm?
- Does your firm have a system for tracking issues and incidents? Is it a centralized system?
- Are most issues self-reported or reported by the second and third lines?
- Does your firm actively track metrics (e.g. KRIs, KCIs and KPIs)?
- What is the frequency of these metrics?
- Are they tracked centrally or across different areas?
- Are they used for decision-making?
- Does your firm have a RCSA program, and, if so, how mature is it?

Parting Thoughts

Risk culture is real and it's measureable. We may not be able to give it a precise numeric score, but we can build programs and track the right information to give some insight into its strength and effectiveness. We need to ask the right questions that benchmark our progress, from where we were yesterday to where we are today.

Improving risk culture is not about eliminating risks but rather having the information to take the right risks to maximize our performance.

I urge you to take this article back to your organizations and start asking the questions above. Document and track them.

Think of new questions to ask and new ways to measure your program's effectiveness. Plot the results in a document over time and, when regulators or external auditors ask about your risk culture, point to that document and demonstrate that you have a strong risk culture!

Ultimately, risk culture is defined by *us* — no matter the tone from the top or guidance from middle management … or even what our colleagues are doing. It is up to us to make the correct risk-based decisions. It is up to us to be ethical and compliant. It is up to us to do the right thing.

*Ryan Rodriguez-Wiggins is a senior director of industry GRC solutions at MetricStream. He previously worked as a director of ERM at E*Trade Financial and as a vice president in the operational risk department at Morgan Stanley.*