WHITEPAPER

3 Talking Points to Identify and Communicate the Good and Bad of Your GRC Program

Risk assurance executives—whether they work in compliance, internal audit, risk management, IT security, or any other related function—ultimately worry about three things as they do their jobs.

- Is everything functioning normally?
- Do I understand how to address anything not functioning normally?
- Am I working effectively with everyone else in the organization who helps fulfill my goals?

Those three questions, for example, invoke all five elements of the COSO internal control framework: risk assessment, the control environment, and monitoring (the first question); control activities (the second question); and communication (the third question). Those questions seek to understand what is normal and abnormal, and whether you can respond to events properly as the need arises. In one way or another, we all ask ourselves these questions every day.

Compliance and audit professionals want to have productive conversations with the CEO and the board along those same lines. After all, senior leadership is just as crucial to the GRC function as you are. James Lam, one of the godfathers of modern corporate risk management, describes the CEO and board as hovering above the risk assurance team in the famed Three Lines of Defense structure: the CEO in the Second Line above compliance, legal, HR, and the rest; the board in the Third Line, above internal audit.

They want the same useful conversations about governance, risk, and compliance that you have horizontally with other parts of the organization; the conversation simply flows vertically, between middle executives and senior. So how should that happen?

1. TALKING ABOUT ROUTINE MATTERS

Boards and CEOs want to know that several types of risk—operational, compliance, financial, reputational, strategic—are understood and managed at the company. Not all of those risks fall under the purview of internal audit or compliance officers, but the key point is what "understood and managed" actually means: namely, that the programs to address those risks are effective. When you are briefing senior leaders at the company about routine matters, to tell them what your program is doing, you really are talking about how effective the compliance and audit programs are (or are not).

Thankfully we have a good sense of what those discussions look like at the typical large corporation. For example, in Deloitte's Compliance Trends 2015 survey, 79 percent of respondents said the chief compliance officer reports compliance violations to the board and executive management; 74 percent report on the status of various compliance issues as they get resolved; 74 percent also report on emerging compliance risks. Sixty-five percent report regulatory fines and penalties, and 63 percent report compliance performance metrics. Two-thirds said they conduct an enterprise-wide compliance risk assessment at least annually.

None of that is to say that compliance is easy. Indeed, any number of reports (including Deloitte's) show that compliance officers are still greatly challenged in their jobs. But percentages that large do indicate that a consensus is emerging on what compliance officers should bring to senior management's attention

Audit executives have a different mission from compliance, and therefore have a different conversation even about routine matters. For example, the audit committee (at most large companies) wants to hear about the audit team's annual enterprise risk assessment. It also wants to hear about the audit team's plans for the year, and how those plans relate back to the company's biggest risks. (Many audit committee charters specifically cite financial reporting risks as something the internal audit function should oversee.) Throughout the year, the committee wants to hear how internal audit works through its audit plan and whatever results emerge.

That difference between compliance and audit is worth elaboration. Compliance oversees risks "in motion" that might range from ethics training to internal investigations or vetting merger candidates. The results of those efforts in any one day or quarter might drive the compliance program's activities in a different direction the next day or quarter. In contrast, the internal audit department's work is (in a perfect world) more planned and punctuated. Internal audit has a risk-based plan, and systematically follows it.

Should compliance and audit talk often to compare the top risks occupying their minds? Yes. Can audit help compliance to determine how well a compliance program is working, and perhaps they present their findings to senior leaders in one voice? Sure. But do they both need to focus on exactly the same risks, and present one unified opinion to senior leaders about risk assurance? Of course not. They play different roles, and support senior leaders in different ways.

2. TALKING ABOUT SENSITIVE MATTERS

At some point, you will need to brief senior leaders about something delicate: an investigation, a high-risk event, misconduct involving other senior leaders, or the like. We should make a distinction here between something specific (say, an investigation into fraud by senior managers), and something that isn't working (too aggressive financial targets or overseas expansion plans fraught with bribery risk). The latter is much more about goals or risk tolerances set by senior leaders that aren't practical to achieve, and we will address that shortly.

For specific problems—well, volumes of literature have been written about how to conduct internal investigations, how to apply attorney-client privilege, when to alert the CEO or the audit committee that a potentially serious risk has emerged. The key points that senior leaders and boards want to know in these situations are these:

If the problem requires investigation, is that investigation being handled properly and securely? That might mean the internal audit team works with the legal department, or hands off the issue to outside counsel entirely. But given the greater odds that some outside party will get involved (the press, regulators, plaintiff lawyers looking to sue), the board will want to know the company is performing its investigation with due diligence.

If the issue is about a high-risk event—anything from a debt-laden merger to a regulatory probe to suspected data breach—has the potential risk been quantified as best as possible? Senior executives will want to know about risk velocity (how quickly things might turn sour) and worst-case scenarios (how much damage, ideally in dollars, could happen). They will also want to know about the chain of control failures that led to something that has happened; or possible control failures for a potential problem, and mitigation strategies the company could implement.

If the problem is a specific senior executive, is the misconduct fully documented? Issues with senior executives breed every sort of headache, from damaged office morale to litigation to lost customers. Taking action against senior executives is a delicate situation and boards will want every assurance they have all the information they need to make the necessary decision.

3. TALKING ABOUT WHAT'S NOT WORKING

A third line of conversation with senior leaders—and possibly the most common—is talk about what isn't working well. Sometimes that might be an emerging risk nobody knows how to handle; other times it might be diplomatic discussion of a business idea that will complicate the mission for risk assurance. It may simply be a discussion of how the company's culture and behavior does not match what senior leaders expect, or believe, it to be.

For example, according to one recent survey from CEB, 62 percent of managers surveyed said no, guidance about a company's risk appetite is not consistent with other management guidance about how the business should run; and 53 percent said senior leaders' actions don't match the risk appetite. Broaching a subject like that with the CEO or the board will never be a fun time, and it is only one example of difficult conversations CCOs and CAEs have with their superiors. One wise move, then, is to anticipate at the beginning: How can we create an enterprise risk management framework that addresses differences of opinions?

Creating an ERM framework that accommodates and resolves differences hinges on setting clear business and risk management objectives (discussed in the first paper of this series), and building feedback loops to generate useful information about your ERM program (discussed in the second paper). Another crucial point is how your control environment—which very much deals with culture, tone at the top, employee respect for ethics, and the like—encourages objective debate. Control activities, workflow processes, reporting lines: they can all change over time along with your organization or business conditions. The control environment touches on principles of leadership and ethical rigor that transcend other, more practical elements of risk assurance. If you have a strong control environment, you have the ability to talk with senior leaders about where risk assurance isn't work as well as it should.

THE PARTING LESSONS OF THIS PAPER CAN BE SUMMED UP AS:

- Senior executives ultimately want to know three things about risk assurance: that everything is functioning normally; that anything not functioning normally is getting the attention it deserves; and how well various parts of the business are working together to manage risk.
- Briefing senior leaders on "routine" compliance and audit matters is a relatively straightforward (if still complicated) process. Briefing them on sensitive subjects requires its own protocols, depending on the problem in question.
- To have productive conversations about how well risk management is faring, companies need: (1) clear business and risk management objectives; (2) feedback loops that generate information about risk; and (3) a risk management framework that can accommodate and resolve differences of opinion—because differences will always arise.