WHITEPAPER

Do We Have a Problem With Compliance Risk Assessments?

By Matt Kelly, CEO Radical Compliance

We have some disconcerting patterns emerging in how compliance risk assessments get done.

PwC's 2016 State of Compliance Report surveyed over 800 compliance officers. Of that group, 77 percent said their companies had some sort of enterprise risk management (ERM) process – and within that smaller group, 88 percent said ethics and compliance risks were part of that ERM process. So if we do the arithmetic, that means roughly two-thirds of all companies sweep their ethics & compliance risk assessments into a greater enterprise risk management exercise. That's one piece of news.

The other piece, however, is that even within that group whose companies have an ERM process – 57 percent of them still do additional ethics & compliance risk assessment of their own. And 23 percent of them say their ERM program doesn't address most of their ethics & compliance concerns.

What's going on there? A few ideas come to mind, and they make me wonder how serious CEOs and boards are when they say they take ethics and compliance seriously.

First we need to cite a point from another PwC study – its Global CEO Survey published earlier this year. In that report, 79 percent of CEOs cited increasing regulation as their top worry about future growth. If increasing regulation is such a concern, then one would assume that compliance officers are getting more involved in strategic planning, right? Who better to provide counsel to the executive committee on that subject than the chief compliance officer?

Except, in the State of Compliance report we see that closer relationship is not happening – at least not nearly to the degree that it should. Only 36 percent of compliance officers said they play a key role in the strategic planning at their business, virtually the same figure as in 2015.

That tells me that many CEOs still see compliance more as a matter of meeting regulatory requirements, rather than embedding principles of good business conduct. And an attitude like that would certainly explain why a company's risk management process would only kinda sorta help compliance, yet still leave plenty of ethics & compliance risks needing their own risk assessment.

ENTER THE RISK OWNERS

One supporting statistic does not an argument make, I know. So let's look at some other evidence elsewhere in the State of Compliance Report.

A crucial goal for any compliance and risk management program is to assign owners to every risk you document. The good news is that 67 percent of compliance officers said their organizations have a process to do that. But when PwC listed 17 different compliance risks and asked survey respondents to say who owned each one at their business, 11 of those 17 risks usually went to the legal department.

Now, I like the legal department as much as anyone – but its primary function is to reduce litigation risk for the company. Which sounds an awful lot like the "meeting regulatory requirements" goal I mentioned above.

What's more, almost all of those 17 risks were assigned to Second Line of Defense functions, from compliance to HR to IT to procurement. The only one that primarily went to operations people in the First Line of Defense was safety & environment. So for all our talk about "the business units have to own the risk," that's yet not happening to a great extent.

That's not proof positive that compliance is still seen as something primarily to be endured, so the company can then get on with business. It does, however, feed into that same inference we can make from the other points raised above. It fits the profile of compliance as a chore, rather than a strategic imperative.

HOW RISK ASSESSMENTS GET DONE

Back to our compliance risk assessments. The survey also found that compliance risk assessments tended to include lots of "top down" elements, as PwC called them: lessons learned from prior compliance failures, results of regulatory reviews, enforcement trends and interviews with management. Much rarer were "bottom up" elements, such as employee surveys or culture assessments.

Those top-down tendencies can carry peril. You end up focusing on the risks you know, or on the issues that your company (or its peers) have already bungled. It's a very regulatory-centric view of ethics and compliance risks, because regulatory requirements are what senior executives know.

What companies need – and what many board directors say they want – is a risk assessment that addresses both compliance and ethics. Ethics risks breed reputation risks, and you won't find a director anywhere who ignores that threat any more. But the worst ethics risks lurk deep within business processes, interlaced among all sorts of other operational risks. So if companies really are serious about taming modern risks that endanger them, a robust ERM process that includes compliance risks is the way to go.

I'm just not quite sure we're doing that.

