

Interview

Kevin Ludwick

Head of Compliance
QUMAS Corp.

BY GLEN FEST

Meeting Regulators' Ends, Not Means, Lowers Risk

Favoring an outcomes-based regulatory environment, former BofA compliance chief and UK regulator says 'principles' over 'rules' makes for better risk mitigation

How would principles-based regulation differ from a rules-based system?

Principles-based regulation is about effectiveness. When a regulator tries to prescribe what a firm can do to achieve the outcome the regulator's [looking for], it embarks upon a long voyage that will ultimately lead to shipwreck. ...[Prescription] is a double-edged sword, because management will look at the bureaucracy that's been created, and say it needs a special SOX compliance program. ...[If] management takes real responsibility for the financial statements they produce, you need them to

take a hard, cold look at the areas of their business most likely to screw up in [mitigating risk] and do something about it.

How can regulation affect decisions?

I know of one institution that pulled out of an Eastern European location because it was concerned with anti-money-laundering risk. ...When it made that decision, what kind of model actually produced that assessment of risk, and what quality of data did it have? The problem with compliance is so much of the work is fragmented. ...But if you can model

and support electronically all the processes that compliance needs to do its job very well, and align that with a risk model, then you're in the game. ...You're able to show the regulator that you can dynamically manage your compliance program, and your perception of risk is informed by your compliance program.

Do regulators see existing shortcomings?

Absolutely. ...If safety means doing everything equally, then it means doing nothing well. And regulators are starting to really understand it.

What will prompt institutions to make adjustments to compliance?

If you look at the speechmaking that's going on from the Fed Reserve board and the SEC, it's about compliance risk management. We write rules on all sorts of things, from market timing to suitability to insider trading to AML...to start looking at this in a risk-based way. Banks can see that. But what banks are struggling with is

[how] to create an enterprise-wide approach that models compliance risk, and to allow that modeling to direct compliance activity to mitigate risk, whether it be in procedures, training, monitoring activity, or investigation.

So is the enterprise risk approach stymied more by data governance or silos?

It's never right to underestimate the shared complexity of any large global banking institution. These things are big beasts to get your head around. And transactionally, the demands of making

money today mean you tend to solve problems in a siloed way. But regulators don't help. They're constantly throwing change at people.

As regulation evolves, how will risk functions change within institutions?

Compliance departments have a degree of work ahead of them to resolve the questions around what the risk model should look like and what compliance processes should be automated and supported electronically in any large organization. [By doing so], they can work across the

complexity of an organization, but will have management teams that are legal entity-based, country-based, product-based. ...The CTO is going to find a demand from compliance to help it become a risk management function. You look at the way other risk management functions work—credit or market risk—it's in real time. We're talking about people who can...develop views of that business to show management and satisfy themselves where the institution is against a given risk file. Compliance can't do that at the moment.

