

November 1, 2008

## Measure for measure

By Victoria Pennington

**(November 1, 2008) Although financial services firms are leading the way in compliance metrics, none has effective measurements in place to allow it to assess how well the compliance department is working, or the levels of risk across its organisation. Victoria Pennington reports**

Alarm bells started to ring when one compliance manager, when asked whether he was using compliance metrics at his organisation, replied he was, but that he wasn't able to say much more than that as his firm had only started looking at this issue "last Wednesday". This response pretty much sums up where the industry is on the subject of compliance metrics.

"The entire compliance profession, even in financial services firms, is in the very early days of compliance metrics," says Richard Cellini, senior vice-president of business and legal affairs at compliance risk consultant Integrity Interactive. "They are in reactive mode, not preventative mode. They are almost entirely organised to react and respond to compliance failures, and are not yet designed to detect, predict and prevent compliance failures."

Too-stringent adherence to the Basel Committee's definition of the mitigation of compliance risks is part of the problem. The Basel Committee defines compliance risk as "the risk of legal or regulatory sanctions, material financial loss, or loss to reputation a bank may suffer as a result of its failure to comply with laws, regulations, rules, related self-regulatory organisation standards and codes of conduct applicable to its banking activities". Many industry sources blame the prevalence of the tick-box mentality on the reactive nature of this definition.

"Most metrics come under operational risk in Basel II, which is all about capturing key risk indicators and key control indicators that show when you are getting to the point of a problem to enable you to undertake remedial action to mitigate it," says Roger Martini-Facio, head of risk and compliance at technology services provider Logica, based in London. "There is no such thing as a compliance metric in the sense of a pre-defined list. There is no real hard and fast rule that says what compliance metrics are. You have to do anti-money laundering - is that a metric? Firms need to show that they are managing risk internally in their organisation. Governance and controls regarding how and what people are doing and what activities/processes are undertaken is where you want to make sure there is compliance. Most banks have only started looking at this more seriously in 2008. Before that they were only ticking the box in regard to operational risk. It is only now the regulators are starting to crack down on demonstrating internal risk management that they are paying attention."

Metrics used by senior managers to look into the compliance departments and assess how well they are working include measuring the number of new regulations implemented within the permitted timeframe; the number of overdue regulatory filings, or remediation of material regulatory or internal/external audit filings; the number of censures, fines and warning by local regulators; the number of internal audit raisings and assessing the management of the regulatory finding - that is, how long it takes them to close off action on regulatory findings. These metrics are fine for analysing how well the function is operating but they do not take into account the interdependencies of compliance issues with other risk areas. Moreover as Richard Pike, product director with software vendor Ci3 in Dublin, points out, because new regulations are of varying complexity, it is impossible to assess compliance in this instance based on speed alone: "It is very difficult to get that sort of performance metric in compliance because the regulations are so different and some are stop-and-start over a longer period. I would say it is impossible to set performance metrics in compliance but you can measure the risk of non-compliance."

Given the recent market turmoil, regulators are poised to become even more stringent in their assessment of a firm's approach to compliance and risk management. Peter Teuten, president and chief technology officer at Keane Business Risk Management Solutions, suggests the current crisis exists partly because of the silo mentality that remains entrenched at most firms, which has not allowed them to see the interdependency of risks within an organisation.

"In banking, the focus on Basel II compliance metrics that look at op risk parameters gear themselves to specific processes within a bank, such as trade exceptions, breaches of liquidity ratios and anti-money laundering," he says. "These elements have been calculated quite successfully by op risk systems geared to key risk indicators and key performance indicators relative to their specific discipline, and are great as far as they go. But the problem is the interdependency of factors beyond the specifics of the silo one is looking at."

A compliance initiative at a firm tends to deal with the need to address issues in isolation - anti-money laundering (AML) for example. But, as Teuten points out, there are many interdependencies of market sentiment and strategic risk associated with AML. "When an AML event occurs, which is in itself a measurable and quantifiable exception to a rule that has been created so that the operational risk can be defined specific to AML, but the interdependency between an AML event and strategic risk, market risk, legal risk or regulatory compliance risk outcomes is not being addressed."

The trouble in the credit derivatives obligations market is just one demonstration of this lack of a holistic approach. The problem of market delinquencies and subsequent writedowns caused the markets to freeze and degrade the value of assets on a mark-to-market basis, which was exacerbated by the reputational risks associated by the re-pricing of assets and writedowns that caused a flight of capital. This in turn resulted in credit rating agencies reviewing portfolios and the creditworthiness of some firms. "So a direct enhancement of what should have been a very linear process of determining the value of assets has been exacerbated firstly by reputational risk and secondly by a credit risk that is market-wide and not specific to one portfolio," says Teuten. "This tells me the compliance initiatives in businesses now are still too rules-based and siloed in their approach."

"The fact is that the interdependencies of risks in an organisation - be they operational risks or market risks - are so intertwined that, unless there is a very clear objective to understand and create the inter-relationship between them, the complexities of the market are such that they will only serve to increase the potential for future catastrophes. This is unless businesses take the opportunity to take a wider view on risk and compliance."

This is where having an enterprise-wide governance risk and compliance platform can help - that's the theory at least.

**"Compliance has become a management discipline and is no longer solely a legal discipline, or an HR and training issue - it is now a risk management control, and GRC platforms are very**

much based on this point of view," says Cellini. "Once you have controls in place, you need to have metrics that tell you how well those controls are performing."

But not many have adopted this approach and those that have are moving at a glacial pace. The breaking down of silos remains a sticking point. "There aren't many companies out there, if at all, that have a compliance department that is completely in sync with the rest of the business," says Zag Asghar, head of performance optimisation application sales for SAP's UK and Ireland services sector, which includes GRC solutions. "This is probably because there are still silos in the company - audit, risk and compliance - none of these has a true version of what is going on in the company. First and foremost, what is really required is a risk and compliance framework. Firms need to collect the bucket of regulatory requirements needed to be addressed, and implement a risk and compliance framework that embodies those requirements. Having done that, they need to ensure they have a single version of the truth - so the risk department, the compliance department, internal audit and, at an enterprise level, senior executives, see the same data. This requires a single repository and a single dashboard but that is the end objective. In the first instance, firms need to be focusing on getting that risk and compliance framework in place, which will give them an opportunity to look at solutions to tackle each issue or consider ways of getting that single version of the truth without ending up with spaghetti associated with disparate point solutions."

Breaking down silos requires much closer collaboration between the compliance, internal audit and risk departments. But this is crucial for getting a holistic view of the risks faced by the company without duplicating information and effort.

Cellini says: "There should be much closer collaboration and co-operation between legal, compliance and internal audit - they each hold a piece of the puzzle, but right now they fear each other and in some instances intensely dislike each other. The legal people know what to look for and the audit people know how to find it and quantify it. That's a marriage made in heaven."

But the tone at the top needs to be right to ensure this occurs. "Creating the metrics for analysis on differing types of interdependent risks requires the involvement of many stakeholders," says Teuten. "It starts at the top, and has to permeate beyond the siloed chief compliance officers into the operational side of the business, to create the ability to communicate, retrieve and disseminate information, and create prescriptive actions that enable a business to be more efficient and run on a best-practices basis without creating impediment to furthering the business."

The problem is that this requires change in a culture that has been in place for decades. "In the past 10 years, 50-60% of risk and compliance initiatives driven down into the business, even from the board level, have been met with suspicion and denial at the operational level," says Teuten. "Unless we treat this process as best practice with a measurable upside to financial performance and align business decisions accordingly, this is going to continue."

There has also been a trend for companies to solve all compliance needs by creating a dedicated department, along with a point software solution. Firms' reaction to Sarbanes-Oxley is a perfect example. In stepping up to the challenges of the new risk-based regulatory environment, companies need to take a more holistic view of compliance, and avoid implementing point solutions to plug a gap. A joined up approach is ultimately what will allow senior executives and boards of directors to look across the entire organisation, across borders, to ascertain where their risks lie to aid strategic decisions. Diluting such detailed information into an understandable and actionable format for boards of directors is a challenge, however. As is ensuring you have the right data to base that information on.

"The communication between chief risk officers, chief compliance officers and their boards of directors has been flawed because of the difficulty of creating compiled information for directors and regulators alike that directors can review and make business decisions on in a matter of minutes," says Teuten. "We do not yet have the magic bullet to enable a compliance officer to say to a CEO not only what they are doing on AML, but also how AML affects the whole business, or

how the related market and strategic risks affect the whole business, and how to make a decision based upon what is happening, what could happen and what the intended outcome is going to be."

Aside from the cultural change required, automating processes is essential to enable a firm to gain a true enterprise-wide view of the compliance risks. A number of software firms have the capability to do this for an organisation. For example, Norkom has evolved its detection technology into a unified investigation framework that enables an organisation to see how effective its investigations on compliance issues were, and how it can be more efficient by automating certain processes. "Within any organisation is a set of operational risks that look down onto the risks the firm faces. The challenge is to visualise that so those at very senior levels in a multi-country financial institution can understand where their compliance risks are, where they have effective mitigation and systems in place, and where they have weakness. They can use this data to build up a view of how they are going to manage those risks over time," says Ed Doyle, senior compliance product manager at Norkom.

Integrity's Cellini points to three compliance indicators that look across the enterprise. One is the analytical assessment of hotline - or any anonymous compliance reporting vehicle - data. "Most companies store this data, which goes directly to the board but it is not really analysed in any great detail," he says. "What a lot of companies are doing is analysing that data and aggregating it to determine what kind of issues are being raised, and in which geographies or business units, to come up with the top 10 risk areas that keep being reported."

The second step after that, Cellini says, is to compare these incidents with the firms' compliance training programmes to see whether there are any obvious gaps across geographies and ensure the firm is effectively deploying resources. The third and final step is to analyse all cases that are pending with law firms - these are essentially compliance failures. By following these three steps based on readily available data, a firm can get a more holistic view of the compliance risks the organisation is facing.

By breaking down the silos and sharing compliance information between departments, financial services firms can aggregate all that data into an actionable format for boards of directors to make strategic business decisions with, which is the ultimate aim. This is a complicated endeavour and cannot be done overnight, but setting out on this path creates a defence for financial services firms operating in a regulatory environment in a state of flux.

<http://www.opriskandcompliance.com/public/showPage.html?page=823692>