

Changing the rules

Speakers at *OpRisk Europe* focused on the challenges brought by rule changes – what supervisors are doing to provide clarity and avoid regulatory arbitrage, and what firms can do to ensure they're ready. **Mark Sands** and **Jessica Meek** report from the conference in London

In June, *Operational Risk & Regulation* hosted its second conference of the year in London. Regulatory change was a focus of attention again this year, with the emphasis on how new high-level laws and directives would be translated into procedures – and the risks and pitfalls in this process.

Bernd Rummel, the principal policy expert at the European Banking Authority (EBA), described the EBA's struggles in achieving Europe-wide rules.

The EBA is pushing to smooth out cross-border differences in the latest Capital Requirements Directive (CRD4), he said, and in doing so, lessening opportunities for regulatory arbitrage.

"It's the initiative of the European Commission to have a maximum harmonisation approach. It is working on CRD4, which will be split into two parts. One part, which is the regulations and is directly applicable, contains all of the Pillar I elements. This will get rid of all the national expressions in the involved areas."

Rummel added there might be some differences in approach to CRD4. "Pillar II and Pillar III will stay in the directive, so there may be some differences in implementation," he said. "However, the European Commission is driving to reduce the level of national expression in that area."

The EBA is working on a standard risk-assessment method, Rummel said. "It is important to have the same understanding of terminologies and definitions on risk. We need to have a common framework for risk assessment." Common methodologies for stress tests and op risk assessments are also being developed.

Rummel added the EBA has also found the practice of peer-group analysis useful. "It is a kind of stress test," he said. "Before we develop decisions, we will look at the industry and see what is going on. Afterwards, where we have issued the guidelines, we will see what the impact upon institutions has been, and if

the guidelines have been appropriately implemented."

As part of its efforts in monitoring systemic risk, Rummel said, the EBA is developing "risk-task boards", which will monitor key risk indicators from multiple institutions simultaneously.

Rummel also mentioned stress testing, a theme that would be popular among attendees of the conference. "Stress testing is also an important task of the EBA. We do supervisory stress testing to build common methodologies," he said. A further task is risk assessment. "If supervisory authorities in the EU do risk assess-

"Many firms are struggling to find the right balance between analysis and reporting for each level of management"

Eric Caban,
Federal Reserve Bank of New York

ments, they also include operational risk. Trying to identify the risk profile of a firm involves how the risk profile is dealt with in risk management and controls."

Marco Moscadelli, head of operational risk at the Bank of Italy, echoed his concerns. He warned of the dangers of regulatory arbitrage – both between countries and between markets. "Risk tends to migrate to less well-regulated areas – is operational risk an example of this?" he asked.

Moscadelli sits on the Basel Committee's Standards Implementation Group for Operational Risk (Sigor), which he said needs to play a key role in setting the framework for op risk regulation. "Sigor needs to define the boundaries of operational risk and other risk types to guarantee a level playing field," he said, adding

that operational risk in particular needs a consistent definition. "Sometimes operational risk losses might not always be reported as such, if profits are low already. It's difficult to identify operational risk – for example, losses to mortgage fraud could be classed as credit risks instead. Banks must reduce the threshold for reporting losses – it should be below €1 million."

New regulations in the US are also pushing financial institutions to step up their internal reporting and stress testing – at least, so regulators hope. But Eric Caban, leader of the operational risk governance team at the Federal Reserve Bank of New York, noted that the improvements are still far from complete, despite the impetus he and his fellow regulators are giving. Caban emphasised that reporting systems can be vital to effective risk management, but that their importance is often neglected within institutions.

"Many firms are struggling to find the right balance between analysis and reporting for each level of management," he said. "It tends to be a mixture of *ad hoc* reporting combined with reporting on the tools already in place. That might not be meaningful."

Caban also criticised business lines' tendency to overly customise risk and control sets. "You have this proliferation of risk and control," he said. "When the time comes to bring all this information together to senior management and have them direct some resources to solving the problems, it becomes difficult."

The framework consolidation stage can be even more difficult, according to Caban. "Banks are creating multiple frameworks in response to various regulatory requirements," he said. "The Dodd-Frank Act is the most significant piece of legislation that the US has had in about 80 years. What sort of legal and compliance risk assessments are you going to have to do to ensure your firm is covered going forward?"

Caban called for an enterprise-wide framework



to deal with this. “I think there needs to be a way to harmonise these disparate elements across the firm to ensure there’s a level of consistency around the concepts and the taxonomy,” he said. “Otherwise you’re going to have a veritable tower of Babel when you try to communicate these results to senior management.”

Caban also discussed the recurrent theme of stress testing – in particular past difficulties with the process. “We saw that in 2008–09, although firms reported enhancement and increased use of stress testing to senior management, gaps remained in their ability to conduct firm-wide tests,” he said. “Key to that was the credibility of the output, especially on the op risk side.”

In the context of Basel II’s advanced measurement approach (AMA), he continued, “stress testing gives you insight into the point at which your op risk model stops working or stops giving you reasonable results”.

New regulation is inevitably going to affect stress testing, he said. “I think the rationale behind stress testing is similar to what we see in the Basel II AMA. The difference in Dodd-Frank is the frequency with which we’re going to expect stress testing to occur.”

Clear reporting brings industry-wide benefits as well as helping the individual banks involved, pointed out Günther Helbok, head of operational risk and risk integration at Bank Austria. His institution is a member of the Operational Riskdata Exchange (ORX), and Helbok led the consortium’s recent work on clarifying standards.

The original reporting standards from ORX had

“We still have to go back to the basics and make sure we are all collecting the same items and we all mean the same thing when we speak about operational risk”

Günther Helbok, Bank Austria

been issued in 2004, and illustrated with examples of how the members of the consortium defined varying losses, dates and event types for reporting.

However, subsequent additions and annotation had become disorganised and confusing, said Helbok. “When the first version of the reporting standards came out, honestly, I thought at the time it was perfect,” said Helbok. “What happened was that over the years we were simply expanding the old documents, slotting things in here and there. We found that, by 2007, it had become a bit difficult to read and that new members of the association were asking more and more questions... We still have to go back to the basics and make sure we are all collecting the same items and we all mean the same thing when we speak about operational risk.”

As part of the re-evaluation of the original document, Helbok said, it became clear some topics needed further fleshing out, having been neglected in the original drafts.

“We had a divergent degree of detail in the document,” he said. “Risk categories and event types were described in great detail because that, in 2004, was still an important thing to think of, and other items were just one page long. So what we tried to do is put all the topics at the same level.”

The document now maintains a consistent structure in each chapter of loss-type definitions, followed by requirements for reporting, which are in turn succeeded by examples and exclusions.

The group concedes the new standards documents will not be final, but Helbok said that, while revisions are inevitable, they should not come around too soon. “Our idea is that this structure will develop in a few years’ time, but it helps us that if additional examples come up, we can simply slot them in or rewrite a requirement or expand a definition.”

Speaking shortly after the conference, Simon Wills, executive director of the consortium, confirmed publishing has already begun, with new information publicly available on the ORX website.

Eddy Wymeersch, former chair of the Committee of European Securities Regulators and chair of the European Corporate Governance Institute, raised the need for clear, functional risk reporting lines, and warned of the need for independence in risk management.

“These days, there is wide agreement that risk has to be structured,” he said, arguing it must be examined at two separate levels. “At board level there has to be a specialised committee dealing with risk, and there

Photos: Murad rm (<http://muradrmphotography.co.uk>)



Bernd Rummel, European Banking Authority

has to be a chief risk officer (CRO).” To be effective, the CRO needs to report either to the board or a risk committee, he continued, and needs to be independent from the operational line. “It’s up to the board to set the risk parameters, not the operations,” he warned.

He also raised red flags over stress testing and risk modelling. Releasing stress-test results might not always be the best idea. “To what extent they should be published is a controversial point. There can be negative consequences, such as over-expectation or complacency,” he warned. Risk models can also be deceptive – as was the case with the Basel II capital adequacy regulations. “One knows how misleading this model can be,” he said. “It can give a false impression of the security of mathematical precisions and reliability. One should always look at the fundamental parameters. Some common sense is also useful.”

Wymeersch also highlighted the dangers of reputational risk, which he said could easily be neglected. “It starts as a small question, but then it develops into a catastrophe. You will never avoid risk coming from somewhere you don’t know,” he said, but added firms should still look at prevention, mitigation and a systematic analysis of reputational harm.

Other speakers warned of neglected risks too – Wolfgang Hütter, head of operational risk at Volks-

bank Vienna, argued business continuity plans (BCPs) need to be reassessed in the light of the financial crisis, and warned complacency could expose business to unexpected and severe risks in this area.

To be truly effective in a crisis, business continuity strategies must be “reloaded” to take into account a wider range of scenarios, Hütter said.

While BCPs have in the past focused on scenarios in which IT and communications systems or premises become inaccessible, Hütter said there must also be strategies for dealing with financial strife. “We found out in the financial crisis that it’s important to have plans for the unavailability of liquidity, and the unavailability or shortage of capital.”

The addition of plans for liquidity and capital management can help an institution develop more effective and holistic BCPs, he said. However, even some of the more traditional systems-focused plans are worth little if institutions are not fully engaged in testing to make sure they are current and effective. “Developing business continuity and crisis management plans is the first thing and it is good to have it. But the second thing is to test it. We do this at least on an annual basis – we test our plans and there are a lot of lessons learned in that phase,” he said.

Plans can always be improved, but flaws will often only be found in a thorough testing process. He gave the example of IT systems failing to function because a password has expired or the system has not been fully updated. “There are a lot of things to do,” he said, “and you will not find them out if you are not testing them.”

Much has been learned in reassessment of business continuity management, Hütter said, noting that institutions should equally strive to understand the unique needs of each discipline. Some departments are able to function without tools that would be considered vital elsewhere, and understanding this is key to achieving efficient distribution of resources in a crisis. “You have to understand your position,” said Hütter. “If you say to me that for two weeks I will have no IT system, that’s not a huge problem. If you say the same thing to someone in our financial markets or treasury department, they will say ‘In two weeks, we are dead.’”

Two other speakers highlighted another neglected area of risk management – the cultural factor. Dean Rowan, chief risk officer at Gulf One Investment Bank, said culture in operational risk management is too often neglected in favour of processes.

“Changing culture means linking performance,

risk and remuneration,” he said. “It’s important to involve human resources departments in operational risk management, because they should be a strategic partner – people are key.”

Adrian Furnham, a professor of psychology at University College London, argued firms can mitigate the risk of employee fraud by paying attention to their infrastructure and culture, as well as to the employees themselves. Many of the characteristics in people who commit fraud are also desirable in the workplace, he argued, citing a competitive nature as being advantageous for employers. Firms must accept these characteristics and look at what they can do with their own systems to combat fraud, he said.

Fair and open infrastructures are the best protection against internal fraud, he said. “Fraud is caused by dysfunctional organisations. One of the issues is management policies and the way in which they’re introduced.” This can lead to embitterment, which is often a contributing factor to fraud, he said.

Recruiting the right people can also go some way to mitigating the risk of fraud within a company. “We do know more about how to select people who are less likely to commit fraud,” said Furnham. “You look for people with the sense of moral right or wrong, with a sense of integrity. You can see the signs in their past.” A company needs to ensure it pays attention to these factors during the recruitment process because the risk of fraudulent activity can be mitigated at this stage.

He added the banking industry is particularly at risk of hiring individuals who are prone to fraudulent activity. “It’s a difficult issue because you want people like that – that kind of competitiveness leads to success,” said Furnham. “The question is when it goes too far.”

But, he added, firms can make efforts to mitigate the risk of fraud linked to corporate culture. “In some senses you can change that corporate culture and make people less viciously competitive,” said Furnham.

Improving security systems might engender fraud rather than discourage it, he warned. “If you introduce security measures into the organisation, such as cameras, are you saying to people: ‘I don’t trust you?’” he asked, adding that the feeling of not being trusted can lead employees to seek revenge, which can result in fraudulent activity.

For more on OpRisk Europe, including our video coverage, go to risk.net/operational-risk-and-regulation