BANCO DE ESPAÑA
Eurosistema

15/11/2019

Opening remarks

11th edition of the European SSM Roundtable/International Bankers Forum

Margarita Delgado
Deputy Governor

Good Morning and welcome to Banco de España for this 11th edition of the European SSM Roundtable, organised by the International Bankers Forum (IBF).

The topic for today's roundtable is the management of non-financial risk. This is an issue which is always in the spotlight and, at the same time, is quite hard to tackle.

The concept of risk is continuously used in banking regulation. A quick search in the CRR1 or CRR2 text will reveal that it is mentioned nearly 1,500 times in each.

Banks are certainly familiar with the regulatory requests to understand, measure, hedge, control, assess, address or mitigate risk. I believe it is fair to say that any firm that has survived the crisis and its long aftermath, without public support, has been largely successful in fulfilling these risk-related tasks. Of course, supervisors are also permanently concerned about risk; to some extent, it is what we are paid for.

Still, I believe both banks and supervisors tend to feel rather comfortable when we assess financial risk. Don't misinterpret me. We are perfectly aware of the consequences that a mismanagement of financial risk can entail, but we tend to look at financial risk in a more natural and intuitive way. Things get a lot stickier when we look at non-financial risk.
What is the nature of non-financial risk? And what makes it different from more traditional financial risk?

The concept of risk is always linked to a loss which is, by definition, uncertain. Any loss which is certain is not a risk anymore; it is simply a cost. Nevertheless, financial risk is always the consequence of specific financial choices; namely, the decision to purchase an asset or grant a loan gives rise to certain risks for the institution.

Despite the uncertainty, the financial risks posed by that given transaction can generally be measured, in the sense that losses tend to be limited and associated with known events, which are likely to occur with a certain probability.

The rationale of banks' business models is to take on this financial risk and generate profit from it. Of course, banks should assess this profitability jointly with the level of risk assumed in order to take informed decisions.

However, the nature of non-financial risk makes it far more difficult for banks and supervisors to tackle. Non-financial risk, whether related to misconduct, non-compliance, IT, reputational, cybersecurity or operational challenges, is not linked directly to financial decisions and has only a downside.

In other words, unlike credit or market risk, here there are only potential losses, which can be large. In addition, non-financial risk can only be reduced or mitigated, but not eliminated, and it is far more difficult to quantify than financial risks.

Despite all these difficulties, or perhaps because of them, non-financial risk has been on regulators' and supervisors' radar for quite some time. In fact, it's been more than 15 years since the Basel II capital accord included a capital charge for operational risk.

15 years later, I believe we can draw two conclusions. First, measuring these risks is still challenging. Second, their importance for the banking business has not diminished a bit. On the contrary, it has become more relevant for banks and, certainly, supervisors.

Indeed, looking at the 2020 priorities, released by supervisors worldwide, it is clear that non-financial risks are on the top of the list. Let me give you a few illustrative examples: the importance of IT has soared, since it has become a key component of any viable Business Model, which makes cyber risk an even greater source of concern. Second, considering recent scandals across the EU I believe I don´t need to emphasize that Anti-Money-Laundering is more relevant than ever. Finally, it is also clear that the nature of retail banking business means that conduct risk is a major source of concern.

In this regard, it is not easy to compile all the losses stemming from the wave of fines and lawsuits that has swept through the financial industry during the crisis and its aftermath. According to a report from the ESRB[1], the cumulative losses to December 2014 stemming solely from misconduct exceeded 200 bn € worldwide, with more than 50 bn € affecting EU banks.

But, despite the size of these losses, the direct financial consequences are not the only source of concern.

Clearly, these losses generally produce second-round effects, mainly through reputational damage that tends to affect the financial sector as a whole, rather than individual institutions. As is currently the case, these losses tend to rise, precisely, in the aftermath of crises, where some of the questionable commercial practices are exposed. Banks are hit by these losses at a time when customers, shareholders and public stakeholders are questioning their business model, precisely because of this risk. Consequently, the upshot could be a clear procyclical effect.

In a nutshell, we must acknowledge that non-financial risk presents certain features that can exacerbate or compound the effect of a crisis. It is also very hard to estimate and, unlike traditional risks, cannot be eliminated; at best, it may be mitigated.

This would be the key question for today: what can we do to mitigate non-financial risk to the maximum extent?

In my view, the mitigation of non-financial risk is linked to the quality of internal procedures, IT systems, governance structure or compliance function of a bank. In other words, it is not so much about what banks should do, but how they should do it.

Naturally, enhancing governance, compliance or IT systems is not easy. It generally involves additional spending that adds pressure to the already beleaguered profitability of the sector. Understandably, some firms see spending in these areas as an additional cost. I believe it is more appropriate to see improvements in IT or governance as long-term investments.

In this context, it is worth noting that we are observing adjustments in business models. Some institutions might need to undergo radical transformation, while others need just fine-

[1] https://www.esrb.europa.eu/pub/pdf/other/150625_report_misconduct_risk.en.pdf

tune their structures. In all cases, we see digitalisation and optimisation of processes, with potential impact on the internal control functions. We also see an increased reliance on outsourcing and an attempt to implement more agile and flexible ways of working.

All these trends imply changes that pose additional risks. In this regard, there are some critical elements that banks need to consider in their management of non-financial risk. Let me say a few words about these elements.

Starting with IT, I think nobody questions by now that technological change should be part of deeper considerations regarding the sustainability of the banking business model in the long term. If we look at what has happened in recent years in other sectors, there is clearly a need for the banking business model to adapt to a new reality.

True, technological adaptation calls in many cases for significant investment in systems to be made. However, such investment today will be key to fostering profitability in the future. A lot of people think that IT change is mainly related to the so-called front-end, namely the customer experience. There is a lot of talk about the interaction with the client and the quality of apps, but I would like to stress that it is even more important to undertake technological change focusing on the back-end processes.

Needless to say, I am talking about client data, which is the basic commodity of this fourth industrial revolution. Importantly, client data is currently controlled by banks, though some recent developments, such as the PSD2 in the EU, might alter this situation.

Accordingly, institutions should strive to make the best out of their current dominant position. Banks should be capable of extracting, exploiting and analysing their customers' data. Management must fully consider this information to take decisions. Otherwise, re-evaluation and transformation of the business model will not be possible.

Therefore, a clear conclusion would be that the business criticality of IT and cyber resilience has also soared, compared to the situation 20 years ago. This makes the investments and controls in this area a key element of the future.

Let me refer briefly to business conduct. The crisis has reminded us, rather painfully, that conduct is another key factor to consider in any sustainable business model. I would like to point out that conduct change is the only means of responding to the challenge the sector faces to restore its image and reputation.

Society has changed in terms of its demands of the financial sector, including also higher standards for AML-CFT. The rules governing customer-bank relations have likewise changed. Banks should, therefore, move to respond to the new social and regulatory reality. It is worth recalling that a very positive consequence of this policy is that it increases legal certainty, significantly reducing potential litigation costs.

In many cases, implementing these policies involves a top-down cultural change. This kind of change is doomed to fail unless there is full commitment and support from banks' senior officers and management. Indeed, without adequate governance and a clear 'tone from the top' there is no chance of success.

As I like to point out in many of my interventions, governance is always a precondition for any significant change to occur within an organisation, but of course it is just a precondition. Evidently, other elements must be implemented in order to tackle appropriately the management and control of non-financial risk.

One initial element relates to the involvement of the Board, which should consider non-financial risk management as part of their regular monitoring, instead of simply reacting to emerging issues if controls fail. Just like in the case of traditional risks, the Board must include non-financial risk inside their risk appetite framework; obviously this implies that they should be able to understand the nature of these risks, in order to discriminate and rank their importance.

Of course, the role of the Board cannot function without the right input from both first and second lines of defence.

In this regard, it is important that, apart from owning and managing risk, the first line assesses key infrastructure areas, such as IT and operations, where most operational failures occur. The culture of the bank should also emphasise that first-line areas should also take responsibility for non-financial risk management, rather than focusing entirely on revenue or cost management.

As you know, the second line establishes the control standards and monitors adherence to them, encompassing risk and compliance functions. Nevertheless, other areas, such as legal, human resources or tax, may also be included, in order to ensure that their expertise in these areas is considered by management.

There is no one-size-fits-all approach for the division of tasks between both lines; but the identification, assessment, validation and reporting of risks and controls should certainly be clearly assigned in every organisation.

As I mentioned before, it is very hard to measure these kind of risks precisely; nevertheless, banks should include qualitative and quantitative key risk indicators in their integrated management information system. To achieve this integration, all parties must speak the same language, which implies applying common taxonomies with clear definitions and indicators per type of risk.

Last, but certainly not least, I wanted to emphasise the importance of having an adequate internal audit as the third line of defense. The role of internal audit is key to challenging the adequacy of the first two lines, underpinning the whole framework.

Let me conclude.

The losses experienced during the crisis and its aftermath should act as a powerful reminder that we cannot relax or lower the bar. There is no room for complacency if we want to avoid repeating past mistakes.
In this regard, I wanted to convey a few messages today. First, maintain your fundamentals and keep on improving your three lines of defense; make sure that accountability and

ownership for each risk is defined and well-understood within your institution. Second, remember that improving essential risk management and controls, including data quality, should not be seen as a cost, but as an investment for the future. Finally, keep on working towards appropriate balances between risk and reward, making this sustainable over the cycle.

I believe it is revealing that the title of the conference refers to the management of non-financial risk as 'the next big challenge'. As I have noted today, these risks have been in the spotlight of banks and supervisors at least since Basel II, so an observer may question whether they can still be characterised as the 'next big challenge'.

I actually agree with the statement made in the title. The pervasive and ever-changing nature of non-financial risk turns it into a permanent challenge for banks and supervisors. The most recent and obvious example would be the emergence of environmental risk as a source of concern for all of us.

Indeed, there is still a lot of catching up to do, so I look forward to today's discussions. I wish you a very successful conference.

Thank you very much.