

**ASHK Risk Management Regional Conference
31st January to 2nd February 2010**

“Guide to an ERM Risk Map and Working in Practice”

Workshop Facilitators:

Mrs Edith Pfister

Mr Robert Chen

Ms Iris Lun

Case Study

Background

You joined ABC Financial Services Company as their first Chief Risk Officer (CRO). ABC Financial Services Company is a global organization offering financial services products in its key markets in over 30 countries. The head office is located in the United States and its shares are listed at the New York Stock Exchange.

You are employed by a subsidiary of ABC Financial Services Company. The regulatory regime in your country is more mature and enforcements are applied in a much stricter manner than in the USA. By way of comparison, the regulatory regime is similar to the one in the UK.

To date Enterprise Risk Management (ERM) has not gained a lot of traction from Senior Management and consequently there is close to nil risk management guidance from head office. Although, under the guidance of head office the company has developed an economic capital model, risk awareness is otherwise rather immature, with the widespread perception that risk management is a 'non-value add' compliance task.

The CEO recognizes the need to develop the risk management framework beyond capital management but doesn't know how to lead or implement such an initiative. He is particularly keen to have greater understanding of the operational risks, their interrelations and their relevance to executing the company's strategy. You have been tasked to address this issue by way of developing an ERM framework.

Challenge

As the company's global reach extended and regulatory requirements proliferated, so did the company's vulnerability to an array of risk challenges. Following an in-house, Enterprise Risk Management (ERM) review, the company identified significant challenges, including establishment of a Risk Management Framework and a Risk Management Strategy, establishing and maintaining a risk register with accountabilities for risk and control, and development of procedures for consistency in risk management and internal control activities.

Legal and regulatory requirements are driving the need for a more robust approach to risk management. At the same time, the CEO and the board want to have a 'complete picture' of the company's risk profile.

The recognition of the fact that much of company's risk exposure was not discussed, yet little alone covered under a risk management framework, led the CEO to look for an innovative comprehensive yet tailored solution that could help them identify the gaps or inefficiencies in their risk coverage.

Task

In collaboration with your team produce/discuss the following:

- a) list the areas involved in risk assessment and management;
- b) discuss approaches for the development a comprehensive risk management framework;
- c) document/discuss the development of a risk register and note the identified key risks in your template with ratings for inherent risks. Seek to identify current and future risks;
- d) discuss/document controls and control effectiveness for each identified key risk in the register;
- e) develop a plan(s) to help close the gaps and to strengthen the framework overall
- f) debate: Who is/should be responsibility for enterprise wide Risk Management? What are the essential skills? How is today's actuarial profession equipped to master these challenges? What must change?

Key guiding questions:

"What are the circumstances under which the firm will fail or have inadequate results/outcomes? What can the company do to improve the quality of management information to make appropriate decisions and minimize misjudgments?"

Tools & Preparatory reading

Worksheet templates will be provided during the workshop and collated at the end of the session for distribution to all participants.

In the appendix to this document you will find a speech held by Hector Sants, Chief Executive, FSA (UK). Depending on experience this document may serve as a reference point to cover the various aspects of Enterprise Risk Management.

Other risk management guiding principles for consideration:

- Risk management creates and protects value
- Risk management is an integral part of all organizational processes
- Risk management is part of decision making
- Risk management explicitly addresses uncertainty
- Risk management is systematic, structured and timely
- Risk management is based on the best available information
- Risk management is tailored
- Risk management takes human and cultural factors into account
- Risk management is transparent and inclusive
- Risk management is dynamic, iterative and responsive to change
- Risk management facilitates continual improvement of the organization

Appendix

The regulator's role in judging competence

Speech by Hector Sants, Chief Executive, FSA
Securities & Investment Institute Conference 2009
7 May 2009

Good morning and thank you for inviting me here today. The FSA has reviewed the causes of the financial crisis and laid out its proposals for the required changes in the Turner Review and accompanying Discussion Paper. It is not my intention to repeat that analysis today. What I intend to do is to focus specifically on the shortcomings exposed by the crisis in the governance and risk management of regulated firms.

From my perspective, it has been demonstrated that firstly, albeit with the benefit of hindsight, there are some management decisions that have revealed a degree of incompetence, and at times a rather cavalier approach regarding risk management; secondly regulators must be careful not to place excessive reliance on senior management judgements; thirdly, the necessary challenge was missing from governance structures, in particular boards, and finally there may well be questions that can reasonably be asked about the openness and thus, arguably, the integrity of firms dealings with regulators, shareholders and their customers.

Sir David Walker, as you know, has been commissioned by the Government to produce a report on governance which will no doubt address many of these critical issues. The FSA is working with him as he develops proposals to address these issues and my comments today are intended to provide insight into our input into that report.

I intend to focus my remarks today, primarily, on the changes we are intending to make in this area and in doing so I will seek to answer: **what is the FSA's role in judging competence.**

I would like to start by explaining how the FSA's 'intensive' supervisory approach is critical to achieving greater effectiveness in this area, discuss with you what this means in practice – particularly for non-executive directors (NEDs) and executives – and finally emphasise how we are enforcing against these issues.

As I mentioned, I have recently laid out the FSA's change in regulatory philosophy and supervisory approach. I might add that I personally feel very strongly about this more intensive approach to supervision. It was always my intention to carry through such a change on taking the CEO role in July 2007; although we have undoubtedly modified this approach in the light of recent events.

I do not intend to repeat the detail here, but I do feel it is worth reiterating a few key points pertinent to examining our role in judging competence.

The historical philosophy was that supervision was focused on ensuring that the appropriate systems and controls were in place and relied on senior management to make the right judgements. It was not seen as a function of the regulator to question the overall business strategy of the institution or, more generally, the possibility of risk crystallising in the future.

As I said in my opening remarks, this financial crisis has demonstrated that we can no longer rely on senior management judgements. In future, therefore, we will seek to make judgements on the judgements of senior management and take action if, in our view, those actions will lead to risks to our statutory objectives.

This by no means weakens our fundamental view that firms' senior management carry primary responsibility for their actions and their resulting consequences. This responsibility is shared with NEDs, shareholders and auditors. Indeed, there are limitations to what regulation can achieve and all regulatory judgements carry risks. I still strongly believe, therefore, that a key element of successful regulation is to work in partnership with these groups. It is only by doing so that we will effect changes in behaviour.

The final point worth repeating here, is that in order to see the full picture of our regulatory philosophy and supervisory approach, it is important to see the linkage with our proactive approach to enforcement – 'our credible deterrence philosophy' – of which I will expand on later when I explain how this fits in to our role in judging competence.

One other point I would like to mention, before moving on to discuss what this means in practice for NEDs and executives, is to reassure you that any changes in this area are being considered within the FSA's wider programme of regulatory reform – outlined in our Turner Review and associated Discussion Paper. We are mindful that our actions need to be proportionate and cognisant of European debates and that they do not cause any unnecessary negative impacts to the competitiveness of the UK financial services industry.

So, turning to the 'regulator's role in judging competence': what does this mean in practice for NEDs and executives?

Evidence from the current crisis indicates that some NEDs have struggled to fulfil their role of providing strong independent oversight of the executive management. The FSA, through our supervisory process will be working to ensure the NEDs of the future have relevant and diverse expertise, have a willingness to challenge, independence of thought and the ability to avoid the 'herd mentality'. This will mean a different calibre of NED, with a different mindset.

NEDs will therefore need to commit to raise their technical skills in order to exercise rigorous oversight. Ultimately, they will need to demonstrate competence with regard to risk management, regulation, and - importantly - the business model of the firm. We do, however, recognise that there will need to be an appropriate mechanism to allow this competence to be acquired which may result in a 'provisional' NED. We will certainly, as a minimum, expect the chairman and senior independent director to demonstrate the full set of competencies.

Clearly, this will require NEDs to work on a more full-time basis and be compensated appropriately. NEDs also need to be supported properly to strengthen their technical expertise. We would like to see greater use, by them, of advisers employed in an independent advisory fashion. Similarly, the Risk Committee should have the ability to co-opt risk experts from outside the firm.

All financial services firms need an effective risk-management function with clear, independent reporting lines to the Risk Committee. Effective risk managers need a combination of technical competence, communication skills (to be able to convey arcane subjects in an accessible way) and stature in the organisation to provide genuine challenge to business managers. This will happen, in my opinion, only if there is an executive director solely responsible for risk on the main board. We need to raise the risk officer up to the level of business unit heads.

More broadly, the key question the FSA expects the senior management of a firm to be able to answer – as I have said on many occasions – is: what are the circumstances under which your firm will fail? We will expect executives to be able to demonstrate their understanding of this and to articulate what plans are in place to mitigate against failure.

In reviewing the recent firm failures, in many cases – albeit with the benefit of hindsight – specific decisions can be seen at the root cause of those firms demise. So what can be done to improve the quality of management decision making to minimise failure?

In many cases, as with NEDs, executives could have greater technical skills and we the regulator should seek to ensure that is the case through the authorisation process.

As part of the Significant Influence Function (SIF) review, the FSA has introduced interviews for candidates for a number of the key functions in an authorised firm. The presumption is that any application submitted by a high-impact firm for the roles of chair, CEO, finance director or risk director will result in an interview. Other SIF candidates may also be interviewed at the supervisor's discretion – for example, if there are concerns about the compliance culture of the firm or the track record of the candidate.

In the first six months of the enhanced approval process, 51 SIF interviews were carried out. In a number of cases applications have been withdrawn following interviews which raised questions concerning the candidate's fitness and propriety. We published a Consultation Paper (CP08/25) in December 2008 which outlines a number of proposed changes to significant influence controlled functions under the approved person regime. We expect to publish a further statement on these alongside Sir David Walker's review on governance.

Supervisors will also be looking more critically at the performance of SIFs especially in high-impact firms. This will include reviewing the competence of SIFs as part of the assessment of a firm's management, governance and culture.

We need to be thoughtful of where we set our required standards but they undoubtedly must be higher than events now suggest they were. On risk, for example, whilst it remains reasonable not to expect NEDs to have detailed quantitative knowledge of risk measurement it is surely reasonable to expect them to have a clear understanding of the nature of the risks and be able to ask the right questions.

Effective risk oversight is more about ensuring the right 'what if' questions have been asked and understood from the business model perspective rather than necessarily focusing on scenarios based solely on historical quantitative data.

Assessment of SIF competence in post will be based around evidence to support the following areas:

- **Knowledge:** Does the individual have and use the generic knowledge of the sector and the specific knowledge of the firm necessary to fulfil the role?
- **Skills:** Does the individual demonstrate the business and interpersonal skills required to fulfil the role and to meet the required standards?
- **Behaviour:** Does the individual demonstrate the attitudes and standards of ethical behaviour required to fulfil their role?
- **Expertise:** Does the individual achieve positive and fair outcomes and meet the performance standards expected for the post?

However, in line with what I mentioned regarding senior management responsibility, this approach does not detract from firms' responsibilities to ensure they have competent people at a senior level.

Delivery of this intensive supervisory approach, and effective regulation in general, can only be achieved in partnership with firms, shareholders and auditors. All involved in oversight must ensure that the right business strategies and behaviours are pursued. A word here on shareholders: I spoke recently at the National Association of Pension Funds conference of the need for greater 'collective activism'. Shareholders must take responsibility to be active individually and more importantly, in collaboration with other investors, to engage with senior management and non-executive directors in companies and question the effectiveness of the construct of their boards. They should also challenge management to ensure business plans are credible.

Before concluding on how we enforce against issues relating to competence, a note of caution regarding some of the issues we need to avoid.

We need, in the changes we are seeking, to create a culture of challenge without creating conflict. We do not want to set up NEDs as a competing governance mechanism against the executive. It is more about making both much more effective. We therefore continue to support the 'unitary board' model, but it must be recognised that such a structure runs the risk of encouraging the herd instinct, both in the sense of encouraging 'follow the leader' behaviour and in the sense of the reluctance to 'break away from the pack' and express an independent view.

I should say that ensuring individuals have the necessary resolve to restrain over-bearing CEOs is undoubtedly a challenge, and I do believe here the regulators have a role in providing support and encouragement. I would expect a key component to be a greater direct communication between NEDs and the regulators. I would also say that the wider corporate community has to be willing to place a premium on such independence.

My remarks on the regulator's role in judging competence would not be complete without an explanation of what we will do when we find evidence of incompetence that has resulted in poor regulatory outcomes. I would like to add, as I have said before, our starting point is that in general we do expect to find market participants who are appropriately experienced and decent.

We thus need a balance to be struck between creating 'credible deterrence' and an environment in which people wish to do business. We will not make judgements based on unreasonable hindsight.

However, as I have said and as I will reiterate here, we will be taking more action against senior management where there is evidence of culpable misconduct.

It's about making individuals realise that they'll suffer meaningful consequences if they break the law and if they fail to improve standards of behaviour. Taking tough enforcement action against individuals, for integrity or competency failures, is therefore a critical component of our credible deterrence philosophy. This is one of the most difficult areas to get outcomes. Cases against individuals are more fiercely contested, the timelines are longer and settlements more difficult to reach. Despite these difficulties, we are committed to holding senior managers to account. I would draw your attention to the fact that the number of SIFs under investigation increased threefold in the last 12 months. Some notable recent cases include:

In the wholesale area, in April 2009, the Tribunal upheld our decision to prohibit Milan Vukelic, the former CEO of a business unit of General Re. The Tribunal concluded that Mr Vukelic 'had overall responsibility for these transactions and chose not to exercise his power of veto to stop what should have been seen to be an obviously questionable deal from going

ahead. In terms of consequences for creditors, investors and shareholders, it made little difference whether Mr Vukelic was dishonest or merely reckless'.

In the retail area, in January 2009, we prohibited the former chief executive of stockbroking firm Pacific Continental Securities UK Limited (PCS), Steven Griggs, and its former finance director, Charles Weston, and also fined them £80,000 and £95,000 respectively for serious failures in the company which led to customers buying high risk shares without suitable advice.

And in the consumer protection area, in May 2008, we fined not only the firm Land of Leather, but also its chief executive – Paul Briant – for failing to prevent mis-sales of Payment Protection Insurance.

A word on how outcomes interact with principles: We would stress that in making judgements on individuals and the consequences of their actions that those judgements should be made in the context of compliance with our principles. In other words, we recognise the lack of principles is often at the heart of wrongdoing.

I might add at this point, that the FSA is practicing what it is preaching. To ensure our supervisors are properly equipped to do this job we have introduced a new Training & Competence scheme which involves a regulatory testing regime for existing supervisors too. We have also ensured that we have the right mix between professional regulators and market practitioners.

In order to address these issues, we as regulators need to work in partnership with all the stakeholders I have mentioned here and with professional bodies such as Securities & Investment Institute. We welcome their voice in leading a debate for change, for example in relation to pushing for change in remuneration practices; on which I have also spoken about recently.

I would like to conclude by emphasising my central point that the structure of governance in financial companies does not need radical overhaul. The attitudes and competence of the individuals who conduct that governance does. In particular we need to create governance arrangements that foster challenge without creating conflict. The effectiveness of governance is the key issue and addressing this challenge is the responsibility of all of us, not just regulators and boards.