GRAS Newsletter 25

August 2010

CRO: hang on to your hat

Summary
The recent banking crisis has put the spotlight on risk management in banks and especially on the way it is organised. In this newsletter, the role of the CRO is discussed in the light of the enhancements to the Basel II framework. The relation between the CEO and CRO in banks merits special attention since, in practice, that relation ranges from strict independence to being joined at the hip. Recent proposals have all pointed in the same direction of a more strict interpretation.

Dear reader,
Can a CEO also be the CRO[1], as was recently suggested by Warren Buffett? Let's see. Broadly speaking, there are three kinds of functions in a bank: business functions, their support functions, and independent control functions. The first two develop organically, depending on the client base, the geographic spread, the product range and market conditions that the bank operates in. To be sure, banks must have policies and procedures in place that stipulate the role and responsibilities within these functions, but the set up and governance is largely up to the bank.

Typically, risk management, compliance, legal and audit are among the control functions singled out by regulators for the third category, that of the *independent* control function. For audit and compliance this independence can be said to be rigorous since it covers all aspects of the work. Not only do they (or their committees) report directly to the board rather than to the executive, these functions are also independent of the business in their day-to-day operations. No business or support function tells audit staff what to do, and vice versa, audit staff in turn are not authorised to perform any operational duties for the organisation. Prior to the credit crisis, risk was gradually drifting away from that model of rigorous independence. Risk and business were becoming integrated. This has now been reversed and risk management is regaining rigorous independence.

But shouldn't everybody be involved with risk management?
Taking risk is what banks do, so it makes sense that risk management is spread around the bank. In that sense, every business owner or process owner is a risk manager. Nowhere has this notion gained greater acceptance than in operational risk, which has made universal risk ownership a central tenet. On the operational level, this does indeed make sense. In their day-to-day decision making, the bank expects everybody to be mindful of the risk/reward effects of that decision.

In this view, an independent risk function is then mainly necessary to develop the methodologies for assessing risks, to ensure the correct application thereof by the business, to verify the use and reporting, and to assign the parameters in the risk applications. If we stretch this world view, the risk function sets the ground rules and the business then uses these best principles and methods to benefit its stakeholders. This is what must have been behind Warren Buffett's thinking when he wrote: "….the CEO of any large financial organization *must* be the Chief Risk Officer as well"

[1] Warren Buffet's 2008 letter to shareholders dated January 27, 2009, page 18. The quote below relates to Buffett's statement that as CEO of Berkshire Hathaway Inc., he himself is responsible for the monitoring of derivative contracts. http://www.berkshirehathaway.com/letters/2009ltr.pdf

CRO: hang on to your hat

The need for independence

There is much to applaud in the idea of a CEO who takes an active interest in managing risk. A particularly strong CEO with the right attitude can be an excellent safeguard. But there are good reasons why banks need an independent CRO and an independent risk function. The main reasons for that is that moral hazard, wilful ignorance, and contrived blindness are unavoidable when risk management and business line responsibilities are mixed - and that includes the CEO level. Of course, the perverse incentives provided by the bonus structure only makes these matters worse. In short, there is a need for a truly independent CRO and risk management function that is properly qualified and staffed and has the ability to exercise objective judgment, regardless of business interests or executive structures.

The regulator's response

The regulatory world has in fact been slow to pick up the strict independence requirement for risk management and CROs. As an example, neither the 2005 BIS paper on 'Enhancing corporate governance for banking organisations' nor the 2006 Basel II document even mention the role of the CRO. This situation changed dramatically after the 2008 financial crisis, when risk management in banks was rigorously reviewed.

The most noticeable effect was in the March 2010 BIS paper on corporate governance[2], superseding the 2005 one. It devotes four full paragraphs to the role and the position of the CRO, stating unequivocally: '…the CRO should also report and have direct access to the board and its risk committee without impediment' and further that so-called "dual-hatting"[3] must be avoided. This call for independent CROs is also reflected in the 2009 enhancements to the Basel II framework[4], which now also explicitly mentions the CRO. Thus, both papers suggest that the CEO cannot also be the CRO, since that would be the ultimate dual hat.

Conclusion

In a perfect world, the CEO and the CRO share identical goals. In practice, CEOs tend to lean towards *advancing* the institution, where CROs lean towards *protecting* it. The same can be said for the business in general versus the risk management function. There is thus great value in a truly independent CRO, with an independent risk management function. The latest proposals from the BIS fully support that notion. It is up to the CRO and the risk management function to show that they have understood and accepted this, and that they are ready to take on the roles and responsibilities that come with being a truly independent control function.

---

[2] *Principles for enhancing corporate governance*, Basel Committee on Banking Supervision, March 2010. On the role of the CRO, see paragraphs 69-72. The risk function is discussed in paragraphs 73-77. http://www.bis.org/publ/bcbs168.pdf?noframes=1

[3] That is to say: "…the COO, CFO or other senior management should not also serve as the CRO", ibid paragraph 69.

[4] *Enhancements to the Basel II framework*, Basel Committee on Banking Supervision, July 2009. On the role of the CRO and the risk management function, see paragraph 19. http://www.bis.org/publ/bcbs157.pdf?noframes=1