GRAS Newsletter 45

April 2012

# A slogan for ORM

and a digression on inherent risk

**Summary**

More than any other risk type, ORM depends on the first line of defence. That is where the cornerstone of managing the bank lies. ORM should therefore be explained to, and be debated with the first line of defence in the clearest possible terms and at every opportunity. Since ORM uses notions that also exist in common parlance, special care needs to taken to be clear about terminology and about what ORM entails. Ultimately, it must be made attractive through its *relevance* to the first line in their course of conducting normal business. If ORM departments manage that, they are off to a good start. A slogan was found to be useful in one bank to reinforce this message to the first line: *All Management is Operational Risk Management.*

**Dear reader,**

All risk professionals know that whatever part of the bank we examine, the real level of OpRisk depends on the business, the first line of defence. Risk management, the second line of defence, can create tools, gather data, analyse, challenge and report but they do not hold the steering wheel on OpRisk. Audit, the third line of defence, can examine and recommend but it is up to the first line (business) to implement and follow up on these recommendations and to actually manage the operational risk. Every ORM training and every ORM conference stresses the same points: managing OpRisk is impossible without engaging the first line of defence. That requires

- Explicit Board commitment;
- KPIs for line management that are risk related;
- Full engagement of all staff.

None of this is possible without clarity of definitions, unambiguous guidelines and frequent reminders of both. That is the first role of the ORM department, which cannot be overestimated. Here are some pointers where to start with this clarification.

**Clarity regarding ORM**

Clarity in ORM starts with clear concepts and terminology. Here, even the simplest concepts sometimes go astray. Take the example of the confusion over inherent risk. Inherent risk is important to create an initial understanding about the nature of the risk in the various areas of the bank, as expressed in a risk map. The risk map is a useful tool to help focus attention on those areas of the bank that carry more OpRisk than others and which require more effort and closer scrutiny. A risk map is meant to be a simple tool, in essence no more than a broad brush view of OpRisk across in the bank based on product mix, process complexity, system dependencies and other business characteristics. This broad brush is necessarily subjective and is in any case no more than a starting point since OpRisk derives largely from unforeseen or neglected circumstances. In OpRisk, the term ‘inherent risk’ was introduced casually to capture risk that simply exists in the bank by the characteristics of the product/process. This casual approach had devastating results. It is up to the ORM departments to correct the misconceptions that continue to exist regarding inherent risk.

A short digression of the misconceptions regarding inherent risk should suffice.

# A slogan for ORM

and a digression on inherent risk

**Deconstructing "inherent" risk**

The term inherent risk is commonly bandied around but is neither necessary nor helpful for the management of operational risk. The usual definition goes something like *The level of risk in the absence of controls*. It is a meaningless but also a harmful concept[1]. It is meaningless because there are no processes without controls. It is harmless because it distracts from what it was meant for. To illustrate this, take the risk of simple theft. Anything short of piling the bank's money in the middle of the street and walking away is a control. Taking it inside the bank is a control, and quite a useful one at that. Putting it in a safe and locking the door is also a pretty sensible and effective control. Locking the doors at night is a another, etcetera.  So what is the (inherent) risk of theft in the absence of controls? About 100% it would seem.

It is harmful, because there is a very useful way to think about risk, which, since inherent is already taken we shall call natural risk. Natural risk follows from the nature of the business, the processes involved, the product characteristics, the systems used, their complexities and extenuating circumstances, all of which are basically unchangeable and unavoidable[2]. This is not so much risk *in the absence* of controls, but risk *irrespective* of controls. As an example, providing credit is by its nature more risky than taking deposits, however many controls surround either activity. How much risk? That is hard to say and I largely guesswork. But in a pair-wise comparison, it is usually quite straightforward to rank order processes, products, departments, even banks by their natural risk. Proprietary trade carries more natural risk than asset management. Unsecured lending carries more natural risk than secured lending. Investment banks had more natural risk than Private Banks. In fact, rank ordering natural risk is child's play compared to assessing risk in the absence of controls.

The ORM discipline would do well to revise all its terminology, programmes and models to see whether they are truly helping the first line of defence in their role of managing operational risk at the coal face. That is, ultimately, the only ORM that really counts.

**Conclusion**

One bank was looking for a slogan for their ORM department. After considering a few that talked about the need for the department to be the bank's conscious, we finally came up with *All management is operational risk management.* That slogan should inspire not only the ORM department but also the first line of defence, where ORM is really managed. That slogan may look like a tautology but it led the bank to the realisation that the first line was insufficiently engaged in ORM. It is hoped that ORM departments address such omissions and use it to bring the message to the first line of defence as well. The idea of a slogan may appear crude or superficial, but if it fits the culture it can work to advance real ORM work in the bank.

---

[1] Note that The ISO 31000:2009 Risk Management standard sees no need to include inherent risk. COSO does state that both inherent and residual risk should be assessed, but fails to supply a reliable method or even a consistent definition for inherent risk.

[2] You might even be tempted to say that this is the true *inherent risk* since no amount of controls can take the risk below a minimum, 'natural', level. Note that this is quite the opposite of the common usage of inherent risk, which is why the term best forgotten and replaced by natural risk.