OPERATIONAL RISK AND INSURANCE – WHAT NOW?

It is now over 3 years since we were confronted with the final Basle II Framework (June 2004) and it is perhaps interesting to draw some conclusions on the current state of operational risk management (ORM) in the financial services industry. We make no apologies for the fact that this summary is perforce partial and obviously based on our own perceptions of what we see and hear from clients and others.

- By and large the majority of clients have gone for the Standardised Method. **We are pleased to note that most have taken a pragmatic approach using organisational structures and basic ORM tools in varying degrees of complexity. It is clear that there is no "one size fits all" model and in most cases entities have adapted to the culture of their institution**. Notwithstanding, maturity of the ORM process varies enormously between banks, with some still only in an initial phase (parallel implementation of MiFID assisting), whilst others are well down the road to an effective embedded methodology.

  Those few that have chosen the Advanced Measurement Approach, often prompted by their National Banks, have had differing degrees of success. When all is said and done we wonder whether presently the additional cost (mainly internal resources) is worth the trade-off for a reduced capital charge. So as not to be contentious we will not discuss insurance implications on capital charge – we will wait and see.

  What ever the method employed, effective Key Risk Indicators (KRI's) seem to present the greatest problem. In short there seems to be no substitute to embedding these in operational IT systems if they are to be reliable and excessive manual effort is to be avoided. This is a time consuming and often expensive task.

- As part of the Basle II process we are now starting to see some more reliable operational loss statistics, although interpreting these meaningfully is still often problematic. It is no surprise that internal/external fraud, professional negligence and operating errors seem to lead the field. In terms of business, Merchant Banking/Trading (errors) and Credit (fraud) seem to be the favourites. There is also little doubt that Internet fraud is a growing phenomenon. **Surprisingly, despite the best efforts of ORM initiatives, loss statistics do not generally seem to be on a downward trend**. Whilst there are numerous possible reasons for this, we would like to believe that it is currently due to the fact that loss reporting systems are still gaining in efficiency.

  In this context, when looking at the root cause of more recent large losses, be they due to fraud or error, we still mostly see the breakdown in simple basic controls at the heart of the problem. In today's environment this is more often than not due to lack of employee fraud awareness, excessive staff turnover and the pace of change within operational processes and organisations. ORM can help by concentrating on the basics and ensuring staff are trained in fraud awareness.

FLUX RISK SERVICES SA – Zandgroeflaan 16, 1160 Brussels, Belgium – TEL : +32.2.725.11.79 - FAX : +32.2.725.17.47
info@fluxrisk.com - http://www.fluxrisk.com

- **From an insurance perspective** there is still no hard and fast rule as to whether the management of insurance is within the orbit of ORM. There are presently as many good arguments for combining the two functions as not. Notwithstanding, when looking at insurance within the context of ORM we would like to highlight some points:

  1. The coordination between ORM initiatives and insurance coverage is still very patchy. Changes in risks or trends highlighted by the ORM process seem to take an inordinate amount of time to feed back into policy wordings, if at all. In part, this is probably dictated by annual renewals but also due to the fact that many organisations are still striving for a more effective convergence between the different strands of the risk "world", notably Compliance, Internal Audit, Risk Management, Internal Control and Insurance. Further, the whole question of operational risk transfer is still in its infancy with respect to limits and deductibles. **When all is said and done the ORM process needs to drive an organisation's appetite for risk and the proportion that is retained or transferred out to the market in one form or another. Also, one sometimes forgets that an alternative is simply avoiding risk!**

  2. As noted, Internet fraud is on the increase with the occasional lurid headlines in the national press of certain countries. Whilst the problem is partly a reflection of the increased use of Internet Banking, it has to be said that individual cases are still relatively small (certainly under insurance deductibles) and mainly stem from the gullibility of individual clients, rather than penetration of bank systems. **Notwithstanding, although a number of specialised "Cyber Security" policies exist, we still find numerous banks insuring themselves under Computer Crime policies that are not adapted**. Good old-fashioned hacking has now been replaced by such delightful techniques as Phishing, Pharming, DOS or BOTS. Unfortunately, third party loss due to denial of service/access (DOS) and the impact on reputation are still largely uninsurable, which may prompt a "captive" solution.

  3. Business Continuity risk has now been on the radar screen since time immemorial. **Nevertheless, we are continually surprised at the number of institutions that still have incomplete, untested or outdated IT and/or operational contingency plans**. Although Business Interruption policies exist and there is definite interest from clients, it has to be said that the take-up has not been as extensive as one might expect. This may be because the primary risk is seen as third party loss, and again, impact on reputation, which are not always covered. Whilst two major insurers have promised new policies shortly, there is really no substitute for a fully documented and tested Business Continuity plan, which is in fact a pre-requisite for valid Business Interruption cover!

FLUX RISK SERVICES SA – Zandgroeflaan 16, 1160 Brussels, Belgium – TEL : +32.2.725.11.79 - FAX : +32.2.725.17.47
info@fluxrisk.com - http://www.fluxrisk.com

4. Insurance (mainly PI and D&O) of the mutual funds business (in house and external funds, investment managers, management companies and attendant directors) still seems to present a major challenge. We repeatedly see that both the insurance industry and banks themselves fail to fully understand the risks associated with the business, which is hardly a new product. **Even some of the newer specialised policies still contain major flaws and we have recently witnessed more than one surprised Assured realise that he has no coverage when faced with substantial losses due to error and/or omissions**. This, due simply to technical flaws in policy wording that did not match the reality of the risk. Just one example to whet your appetite: **how many PI policies have an exclusion covering "the interference of the Assured in the affairs of a client" or similar?** Now assess where you as bank have the majority of directors on the board of a client mutual fund (clue: certain regulatory regimes such as Luxembourg actually *oblige* promoters of funds to have a majority on the boards of such funds).

5. Outsourcing is a growing phenomenon across the industry and we increasingly see entire processes under the control of third party service providers. To our knowledge there is no single policy to cover this risk, rather, certain aspects are sometimes included in PI, Business Interruption or Computer Crime policies. **Short of insuring the risk, there is no substitute for insurance and risk managers ensuring that there is a clear internal policy on outsourcing and that there is an effective process to guarantee that the service provider is himself adequately insured**. This is often easier said than done and should ideally be policed by the insurance manager, as only he has the required experience of policy wordings. For example, care should be taken with service provider policies not written on "an each and every loss basis".

It is perhaps no surprise if we close by saying that ORM (or to use the latest buzzword Enterprise Risk Management) is now on the map, but still has a long way to go before achieving the maturity of the Trading and Credit risk processes. Amongst other, we believe that this will require greater empowerment of Ops Risk Managers in relation to the business itself. Nevertheless, no amount of ORM would have prevented the Northern Rock debacle that appears to be the result of a flawed business model and possibly lack of effective regulatory oversight. Or would it - does anyone remember liquidity limits? But then again that's Trading risk, isn't it?

PATRICK MAUGHAN

FLUX RISK SERVICES

OCTOBER 2007

FLUX RISK SERVICES SA – Zandgroeflaan 16, 1160 Brussels, Belgium – TEL : +32.2.725.11.79 - FAX : +32.2.725.17.47
info@fluxrisk.com - http://www.fluxrisk.com