GRAS Newsletter 53

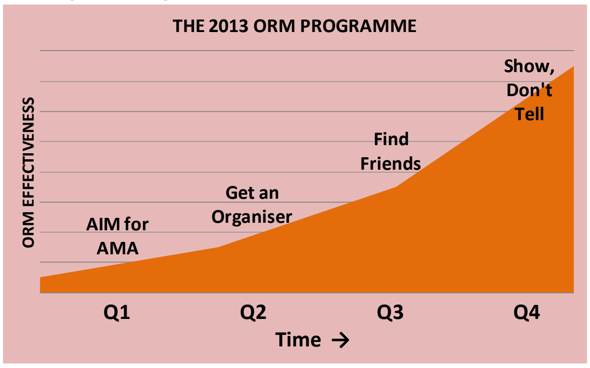
December 2012

An ORM programme for 2013

Summary
There are four clear steps that ORM can take to put itself on the map in 2013. Increase its ambition level, adopt a GRC system, get other control functions to join this initiative and use the GRC to show how risk management benefits the business.

Dear reader,
There must be quite a few OpRisk managers who are secretly pleased with every new fraud case, operational mishap or financial crisis.[1] It appears to guarantee continued attention (and budget) for ORM and it does, indeed, put OpRisk at the centre of attention — briefly. Often, however, ORM fails to capitalise on this position. It fails to deliver the goods[2], thereby disappointing the bank's management which ends up weakening ORM rather than strengthening it.

On a positive note, there is a lot ORM can do to strengthen its position, and there is a lot the bank stands to gain from that. But rather than wait for the next headline, ORM must follow a clear course of action and earn its place under the sun. Here is such a four step plan (for roughly four quarters) that will strengthen the ORM capability of the bank and to help it deliver the goods in 2013.



Step 1: Aim for AMA
ORM needs to have a focus and AMA is by far the best option. By aiming for AMA qualification, banks need to put in place a thorough ORM governance structure and a comprehensive programme. They need to implement this programme with integrity, must evaluate its effectiveness and ensure that the outcomes are used in day-to-day decision making (the so-called 'use-test'). The constant pressure under AMA to clarify and quantify risk, to verify risk levels and to translate this risk level in capital requirements speaks a language the business understands.

The focus that comes with aiming for AMA is beneficial, even if the bank does not put in a formal AMA application. The preparation itself will promote coherence between OpRisk programmes, will force full reporting of incidents and will prompt ORM to evaluate actions in order to adjust AMA scores. The decision to aim for AMA is therefore not a trivial one, since it requires significant investments, but, once taken, it is the first step towards an effective ORM.

Step 2: Get an Organiser
Secondly, and as a corollary to the AMA ambition and the use-test, ORM must be mindful of the data it collects. Countless banks perform risk assessments and gather KRIs that never get combined into a broad risk view. Much work is one-off, kept in word files and spreadsheets, sometimes not even centrally stored. That is no way to manage risk across the bank and over time.

---

[1] In much the same way that each (foiled) terrorist attack benefits the security industry.
[2] Never mind that these 'goods' are themselves poorly understood. Part of the frustration of OpRisk managers is that there are no prizes for preventing fraud or avoiding operational mishaps.

An ORM programme for 2013

A repository of ORM data, with access control, proper data maintenance and reporting capabilities is a must for any bank and indispensible for AMA. That repository should go beyond loss data and should include objectives, risks, controls, assessments, governance structures, limits, and, most importantly, actions and the status of such actions. Now that GRC[3] systems are reasonably mature, the selection process can be completed in a fairly short period.

Step 3: Find Friends
GRC systems work best with plenty of data and luckily, ORM is not the only programme focused on operational risks and controls. Internal Control, Audit, Compliance, BCM, Fraud management, AML, Information security and Physical security are all part of the family of control functions. Each can contribute to the completeness and coverage of the GRC data and without this cooperation ORM is unlikely to get a complete picture of what is going on in the bank.

Step 4: Show, Don't Tell[4]
True OpRisk awareness, in terms of a deep appreciation of the relevance of monitoring risks and controls by the first line of defence, is the best recipe for a sound ORM practice. Achieving such awareness greatly enhances ORM effectiveness and is therefore the ultimate order of the day for risk management. The order of the day for the business, however, comes not in terms of OpRisk awareness, but in terms of cost, revenue, profit and ROE.

Too often, ORM awareness stops at telling the business what the ORM policies and procedures are and when the next KRI submission or Self Assessment is due. With the many pressures the business faces, merely *stating* that ORM is a good thing will not hit home. Rather, OpRisk managers should *show* that sound ORM provides added value (preferably in terms of cost, revenue, profit and ROE). That requires business examples and real cases, analysed in terms of costs, opportunities and actual impact on performance.

A case in point is the loss database. This should be a fountain of information regarding underlying causes, actual impact and improved control measures. But merely telling the business what the losses were in colourful pie-charts is not very inspiring. Showing how the ORM programmes help to bring the losses under control and how that affects the bottom line will inspire the business more than another ranking. GRC systems worth their salt facilitate this use of ORM data.

Conclusion
2013 promises to be a busy year for ORM. With increased regulation, profits under pressure and greater risk awareness, banks are open to better risk management, provided it has its act together. The programme for ORM in 2013 consists of four steps: 1) Aim for AMA; 2) Get an Organiser; 3) Find Friends; 4) Show, Don't Tell.

[3] GRC = Governance, Risk and Control: the catch-all name for repositories of control related data.
[4] A stock phrase in writing classes. To make an image stick in a novel, one should paint a picture which conveys to the reader that John is happy from his actions, e.g. "John was whistling while washing up", rather than simply state "John felt happy this evening".