GRAS Newsletter 34

May 2011

GRC between ICAAP and ERM

Summary
Since the BIS published the *Sound Practices for the Management and Supervision of Operational Risk* in 2003, banks have developed a set of techniques that have become the standard fare of ORM. Despite this rather limited set of techniques, ORM has struggled, and indeed still struggles, how to present the result of its programmes and how to get these outcomes applied in their institutions. Furthermore, it is still looking for the best way to integrate the ORM result with that of other risk types and neighbouring disciplines.
One school of thought tries to achieve this through ICAAP and regards the relation to capital requirements as the best way to incorporate OpRisk data. Another school leans towards ERM, aiming to integrate ORM data with all other risk related data. The middle ground is represented by GRC which looks like the most promising way of using OpRisk data effectively by focusing on ORM's strength, which is its focus on the bank's processes.

Dear reader,
In an attempt to encourage banks to take a holistic view on the risks they are exposed to, various programmes have been launched, such as ICAAP[1] and ERM[2]. These programmes differ radically in many aspects. One of the differences that stands out is their focus. ICAAP, which is concerned with the capital required to ensure each risk is adequately covered, has a very clear focus. It is basically the formalisation of the capital requirements for every risk type. Since in this approach, the risk data is limited to the *effect* of risk on capital requirements, it manages to stay away largely from the risk data itself which is left to the various risk silos.
On the other end of the spectrum, we find ERM, which attempts to integrate all manner of risk data from a content point of view and consequently lacks such a clear focus. There is not a single measure that is the end result of ERM, nor is there a single methodology or framework that supports it. Its goal is, rather, to allow the 'management' of all risks. The problem is, it has failed to actually combine risk data, and in the absence of a coherent focus, a comprehensive methodology or a simple set of measures is has not truly managed to take away much of the silo treatment of the various risk types.

How does GRC fit in?
GRC[3], the topic of this newsletter falls between ICAAP and ERM in terms of focus. It is concerned with the control functions of the institution, gathering information about risks, controls, control objectives, control gaps, recommendations, findings as well as proposed and agreed actions. Typically, GRC is the terrain of ORM, Internal Audit, Compliance, Internal Control, Finance (through Sarbanes-Oxley requirements) and Human Resources departments. The common

[1] ICAAP = Internal Capital Adequacy Assessment Process. The idea of ICAAP is that firms assess the risks for all their business activities and translate that into an appropriate level of capital for these risks.
[2] ERM = Enterprise Risk Management is defined by COSO as a process […] designed to identify potential events […] and manage risk to be within its risk appetite […]
[3] GRC = Governance, Risk and Compliance. This umbrella term actually does not have a strictly defined meaning. In practice it combines the information typically gathered under Operational Risk, Compliance, Audit, and Internal Control programmes into a single repository for analysis and reporting.

GRC between ICAAP and ERM

element among these functions is the focus on the control over the bank's processes. GRC is typically centred around fairly detailed process descriptions to which risks, control objectives etc are attached. One way of looking at GRC is that it is a repository of all process control related data in the institution.

At the same time, GRC can be said to lack singularity of purpose. What exactly GRC is for is not immediately obvious. Is it merely a repository for formal process data, is it an assessment machine, a reporting engine, a collection of loosely related data or is it a one stop view of the bank's risks and controls? Or, indeed, is it the practical side of ERM[4]?

Benefits

The best way to approach that question is to look at the benefits GRC promises and to evaluate whether these promises are attainable, practical and worthwhile. These promised benefits are almost all connected to the fact that GRC operates with the single repository for risk and control data. That leads to better storage, retrieval, data management, access control, workflow and audit trails as well as safeguards for the integrity of the data, the completeness of coverage of internal and external regulations and a robust environment to maintain hierarchies and reporting standards.

Given that OpRisk, Audit, BCP and Compliance have a shared object of study, namely the bank's processes and the risks and controls inherent in these processes, there is no reason why such a repository would be unattainable. Next to that, it must be said that it is practical only if the relevant departments are willing to let go of their silo approaches and actually share risk and control data. In some banks that will be a significant hurdle but it is by no means impossible. Lastly, the question is whether these goals are worth the investment. GRC platforms are rapidly evolving towards a common standard but still demand a significant investment. But the fact that GRC makes it possible to do away with the fragmentation of the systems currently in use for ORM, Audit etc, the many in-house developments as well as un-maintainable spreadsheets is a plus. At the same time, GRC should save labour, maintenance and duplication costs and is actually unavoidable for banks that want to follow best practices.

Conclusion

The imagery typically used in GRC presentations resembles a pyramid with the institutions' processes and governance structure at the bottom, overlaid with risk and control data, followed by all manner of assessments and topped by various reporting engines. Although this is an idealised picture, it pays to take note of it. Unlike ICAAP, GRC does not lead to a single monetary number but rather to a wide range of reports. At the same time, it is also not as undefined as ERM often is, since the object of research is restricted to risk and control data. That may turn out to be the biggest strength of GRC. And if it sticks to what it does best, it may be the best thing that happened to OpRisk since its official endorsement under Basel II.

[4] Or would that be IRM, as some people insist on calling practical ERM. In that view, IRM = Integrated Risk Management. All this alphabet soup is regrettable and the whole concept of IRM may just be ERM having a mid-life crisis. So far, it has not developed a separate methodology or a specific object of study.