GRAS Newsletter 60

July 2013

ORM & Audit: A Matter of Distance

Summary: Superficially, ORM and Audit have much in common. Both are focused on risks and controls, both are looking to identify weaknesses, and both are often seen by the business as a necessary evil. There are, however, significant and important differences. Of the four differences between Audit and ORM, the most complex one is ORM's proximity to the business. ORM, acting as an independent business partner, should enable the first line of defence to identify and mitigate deficiencies ahead of Audit reviews. This partnership can only work if ORM possesses superior business knowledge, can fall back on a clear risk appetite statement and is backed by a strong CRO. As a bonus to the first line of defence the identification and mitigation of deficiencies through self assessments, *ahead of Audit reviews*, will go a long way towards a favourable Audit rating on the bank's risk management capability.

Dear reader

The business as well as the senior management (and occasionally auditors and OpRisk managers themselves) are sometimes confused to the point of exasperation about the role of Audit versus that of ORM. They have the same mission, right? They do the same things, right? They produce the same type of output, right? They cover the same ground, right? Well, up to a point. We will identify four aspects where Audit and ORM differ and explain how that difference can be exploited to ensure good governance and a well-managed bank.

Aspect	Operational Risk Management	Audit
1 Purpose	To assist the business in managing its risk within the bank's risk appetite	To provide an independent, objective assurance function and advise on best practice
2 Risks	Focus on (specific) Residual Risks	Focus on (generic) Inherent Risks
3 Contact frequency	At least quarterly	(Bi-)annually as per Audit plan
4 Business proximity	Close, allowing for short communication lines, swift response and early identification of emerging risks	Distant, allowing for fierce independence and objectivity

Table 1. The four major differences between Audit and ORM

1. Different Purpose

The ultimate goals of all bank activities may be shared, but the immediate purpose of Audit and Risk management are miles apart. Risk appetite in itself is of no concern to Audit. Their guidance comes for their professional judgement regarding: effectiveness and efficiency of operations; reliability and integrity of information; compliance with laws, regulations and contracts and of the safety of the bank as a whole. Risk Management, in contrast, aims to increase enterprise value through the careful understanding and management of risk. The assumption of financial and non-financial risks, *within the bank's appetite*, is an integral part risk management.

2. Different approach to Risks

Inherent risk is a major starting point in putting together an Audit plan. It ensures that material risks will be examined and is in line with Audits independent role. They will decide what risks matter. For ORM, however, *residual* risk forms the starting point of assessments. These risks are compiled in close cooperation with the business, and are central to the ORM efforts. The surest way to make the business buy into the risk register and risk programmes is to focus on the residual risks which are observable, rather than on theoretical inherent risk.

ORM & Audit: A Matter of Distance

3. Different approach to Contact frequency
Whereas Audit descends on the business in an annual or bi-annual schedule, ORM typically sits with the business on a quarterly or monthly basis. As the second line of defence, ORM is an extra pair of eyes and that can only function well if keeps its finger on the pulse of the business. Although by no means part of the day-to-day operations, the dialogue between business and ORM demands a frequent status update on (emerging) risks.

4. Different approach to business proximity
Risk Governance is often presented as a set of concentric circles, with Audit as the outer circle, the business as the core and Risk Management in between. This image correctly suggests the relative distance between Audit and the business and the relative proximity of ORM to both. One consequence of this extra distance between Audit and business is that Audit can be fiercely independent. ORM does it by persuading the business to step into the risk manager's shoes – a softly-softly approach. Audit does it by checklists, observations, sample testing leading to an independent opinion and rating – a stern approach.

The relative proximity of ORM to the business brings some advantages and disadvantages. The disadvantage is that ORM risks becoming part of the business, which is clearly wrong. ORM must always keep an independent reporting line through the CRO and must be in a position to challenge the business. But it would also be wrong to play that card recklessly. In fact, the advantage of ORM and business as a partnership is that it allows both to identify risks, vulnerabilities, weaknesses and deficiencies *ahead* of Audit. In fact, issues that were identified and addressed through a self assessment programme should count positively towards management's capability in the next Audit.[1]

Conclusion
Control functions share an ultimate goal, but they achieve it through different means and by playing different roles. Crudely speaking, ORM and Audit act as a good cop–bad cop team in managing risk. Both approaches have merit and both can be overdone. The proximity (and hence the dependence of ORM on the business's cooperation) is both its strength and its weakness. Weak if the closeness leads to a failure to challenge, but strong where it manages to make the business appreciate and take ownership of its risks. One thing, however, should be clear. If ORM loses the proximity to the business it also loses it added value and it becomes a nuisance. If ORM can capitalise on its proximity to the business, it will add value to the firm by timely addressing issues, thus avoiding losses and relieving Audit at the same time.

[1] Consider two geographically separated business units with somewhat identical products, processes and clients. Both BUs execute the same ORM programme. BU-1 has identified ten risk issues, eight are high risk issues with an action plan and two are low risk issues that have no action plan as yet. BU-2 has identified zero risk issues and hence no action plans. All other things being equal, if you had limited Audit resources, which unit would you visit first?