GRAS Newsletter 14

September 2009

Getting the most mileage out of RCSA

Summary
This newsletter is concerned with the most commonly applied ORM tool: Risk and Control Self Assessment (RCSA). It is one of those ORM tools that comes with a fundamental handicap: that of assumed understanding. Here is a brief discussion of five of the misunderstood aspects which will help to combat this complacency and that will help banks get the most mileage out of their RCSA programmes.

Dear reader,
Risk (and Control) Self Assessment is one of the cornerstones of many bank's ORM practise. It has benefitted from the explicit endorsement in the Basel II programme as described in the "Sound Practices for the Management and Supervision of Operational Risk" of 2003.[1] It has indeed proved to be a versatile tool, and has been deployed at various levels in many organisations. Apart from versatility, its enduring appeal is equally due to the fact that RCSA is one of the most efficient ways of engaging staff, uncovering risks, and develop solutions. After nearly 10 years, we can take stock and to take a look at the state of RCSA and how it may be put to the best use. Five aspects to consider are: Focus, Timing, Ownership, Reporting and Continuity

A. Focus: Is this about Risk, Control or Risk&Control?
Controls are there to manage risks, and thus the two are inextricably connected. Their characteristics, however, could not be more dissimilar. Risk is concerned with all manner of probabilistic events and is hence limitless in scope and uncertain by nature. Controls, on the other hand, concern *known* actions or process steps and can thus be listed comprehensively. Both have their uses but it is important to have different tools for different purposes. Combining tools for the examination of free format residual risks with tools for the evaluation what is known serves neither.

In RSA programmes, controls merely function as signposts in the workshop, brainstorm or scenario development process. The control lists are there as background information. To develop new actions, however, far more importance is given to examining 'causes' or possible circumstances that may affect the process. RSAs are typically used to develop additional controls, rather than evaluate existing ones.

In CSAs programmes, it is all about efficiency and effectiveness, with risk playing the role of background music. The approach is typically questionnaire based or walkthrough. These programmes help decide which controls need strengthening and which controls are superfluous. CSAs are thus great for evaluating existing controls, rather less useful for developing alternatives.

[1] Paragraph 25 states: 'Amongst the possible tools used by banks for identifying and assessing operational risk are: • Self- or Risk Assessment.' Note the subtle 'or', which many ORM professionals conveniently ignore.

© 2009 GRAS B.V.

Getting the most mileage out of RCSA

For maximum effect then, RCSAs should be executed in separate RSA and CSA programmes, here called R(C)SA, focusing on different aspects and following separate implementation paths.

B. Timing: When is an R(C)SA in order?
RSAs and CSAs make the most sense in relatively stable environments where participants can be expected to be interested in improving the business process. Both aspects need to be in place for a successful self assessment. Since these tools capitalise on (subjective) opinions regarding *existing* practice, the opinions are much less relevant in developing situations. In such circumstances, the participants are likely to have their own agenda's.

As to frequency, CSAs can be executed with a much higher frequency than RSAs, since a checklist gains from repetition while a brainstorm / workshop discovery process suffers from quickly diminishing returns.

As a rule, RSA should not be attempted more than once a year, whereas CSA can comfortably be executed on a quarterly or even monthly basis. Either is best done in stable environments.

C. Ownership: Whose assessment is it anyway?
The popularity of RCSAs may in part be explained by the word "Self". A cynic may observe that it has allowed weak ORM departments to dodge responsibility for the quality of the programmes. In fairness to struggling ORM departments, many RSA methods stipulate that ORM should act as *facilitator* to the staff undergoing the RSA. Experience shows that a facilitator who understands the business, the processes, the exceptions, the informal culture, the formal controls and the environmental challenges is not a luxury but a pre-requisite for a successful RSA.

R(C)SA, by definition, should reflect the opinions of those who are directly responsible for the execution within the business unit, process or product under investigation. At the same time, the responsibility for the quality of the R(C)SA rests with the ORM team.

D. Reporting: Who needs this information?
A common response from managers after an R(C)SA is: "This is not telling me anything new". This is a serious problem for ORM departments, since it may discredit the whole ORM effort. An R(C)SAs that focuses on mere risk description, impact and likelihood estimates or control box ticking is indeed not worth the trouble. The added value of best in class R(C)SAs is to go way beyond that level, focuses on improvements and is only truly successful if management perks up and takes notice.

Unless R(C)SA results are relevant for management (decision making), the exercise is no more than an expensive awareness tool.

© 2009 GRAS B.V.

Getting the most mileage out of RCSA

E. Continuity: What do we do the next time round?

For CSA, repetitive sampling provides a better insight in what controls work well. It thrives on repetition, since that shows how controls behave and what effect they have on the overall risk position.

For RSA, however, the second time a unit, process or product is tackled requires a different approach. Many banks are at a loss what to do once a unit or process has been subject to an RSA. Once the risks have been identified, scored, impact and likelihood estimated have been obtained and some actions have been defined, what is there to do the second time around?

Typically the second round of RSAs takes place after one or two years. During the period, a wealth of risk related information have come to light, ranging from loss data reports, KRI analysis and CSA output to audit reports and new product information. The updated Risk Register, which by then should mirror the actual risk profile is commonly used as a starting point for the second round of RSAs. This shifts the primary focus of RSA from risk identification to risk assessment, which allows for an increased focus on (effectiveness of) controls in the R(C)SA.

The future of Self Assessments

Due to the high degree of flexibility and openness, RSA remains an extremely valuable tool in the ORM toolkit. It allows risks to be identified and thrives on creative input. CSA forms a natural, complementary tool to RSA by providing up to date information of the functioning of controls. CSAs, however, only deliver this information when they are executed in a strict format and at a higher frequency than RSAs.

As far as next steps go, RSAs are more likely to change than CSAs. RSAs (while always aimed at developing actions plans) follow a different path to that goal over time. They start out with a view towards risk identification and over time (say after one or two years) can be shifted towards more continuous risk assessment. Once that stage has been reached, the two assessment programmes CSA and RSA may develop into a properly merged RCSA programme. Few banks are at that stage today.

© 2009 GRAS B.V.