GRAS Newsletter 22

May 2010

Nine steps to making risks MECE

Summary

The risks in Operational Risk management are manifold, ranging from theft to mistakes and from faulty product design to poorly motivated staff. When we define and classify risks, there are two objectives: we want to avoid double counting and we do not want to miss important risks. This is sometimes called making risks MECE. "MECE" is an acronym meaning "Mutually Exclusive and Comprehensively Exhaustive. This memo gives some guidelines developed by GRAS to help create a MECE set of risks from a given generic list of risks that may not be MECE.

Dear Reader,

Operational Risks come in many different guises. Exaggerating only a bit, the lists of risks sometimes resembles the famous opening line in Borges' well known taxonomy for animals[1]. That consists of 14 classes of animal, divided into: Those that belong to the Emperor; Embalmed ones; Those that are trained; Suckling pigs; Mermaids; Fabulous ones; Stray dogs; Those included in the present classification; Those that tremble as if they were mad; Innumerable ones; Those drawn with a very fine camelhair brush; Others; Those that have just broken a flower vase; Those that from a long way off look like flies." This newsletter proposes a method to ensure that the list of operational risks do not end up resembling this list of animals.

Characteristics of risks

By definition, a risk is the existence of the probability that an event occurs. Since the number of possible events is limitless, the number of risks is vast. To keep the number of risks in scope manageable we group or categorise risks that share particular characteristics. The Basel II framework has classed events[2] in seven categories. These categories are often useful, but they are not the best example of a MECE system[3]. Because it is useful to have a common classification, we shall continue to map risks to the Basel event categories for grouping purposes, but we will also add a three dimensional model to ensure that our risks are nevertheless MECE.

The three dimensions are:

- Process (fixed)
- Cause (variable)
- Setting (variable)

One of these dimensions is fixed, i.e. we know all its possible values. Two are fundamentally variable, meaning that we can never enumerate all possible values.

---

[1] "The Analytical Language of John Wilkins", by Luis Borges , 1942. The list is supposedly taken from "the Chinese encyclopedia *Celestial Emporium of Benevolent Knowledge*.

[2] Note that the Basel II documents classify Events, not Risks. There is an important difference. Since, *by definition,* events have actually occurred and are therefore observable they can be analysed with much more rigour than risks, which, as *probabilities* of events, are mere abstractions.

[3] The Basel II classification is not of the same class as Borges' example, but it is certainly not MECE.

Nine steps to making risks MECE

The process dimension

For the process dimension, it is worthwhile to create specific risks for each one, i.e. for each process. Consider a generic risk, such as “The risk of processing errors”. While this risk exists in all processes in the bank, it adds little value. For specific processes, e.g. client account opening, however, we can be less generic and describe the risk as “The risk of incorrect recording the client’s full address”. That is a more meaningful risk, since it provides pointers where to look for it, and also what to do about it. So to make our library of risks MECE, we should create specific risks for each banking process.

The cause dimension

A cause is defined as a prevailing circumstance that increases the probability of an event, in other words, that increases risk. Any risk will have a range of causes, each of which increases the probability of that risk occurring. These causes are the best starting point regarding what to do about the risk, how to tackle it. To make the risks MECE, we need to acknowledge that if the causes that lead to the risk are similar, then the actions taken to mitigate the risks will also be similar and therefore the risks can be grouped without loss of information.

The setting dimension

Apart from causes, which increase the probability of an event, countless other circumstances define the risk profile. That could be geographic location, product range, IT infrastructure etc. Even if a bank has a single process, there may, e.g., be differences in IT infrastructure between countries. That may lead to different specific risks, although the generic risk can still be the same. It is worthwhile to be specific in these cases. These sets of circumstances we call settings.

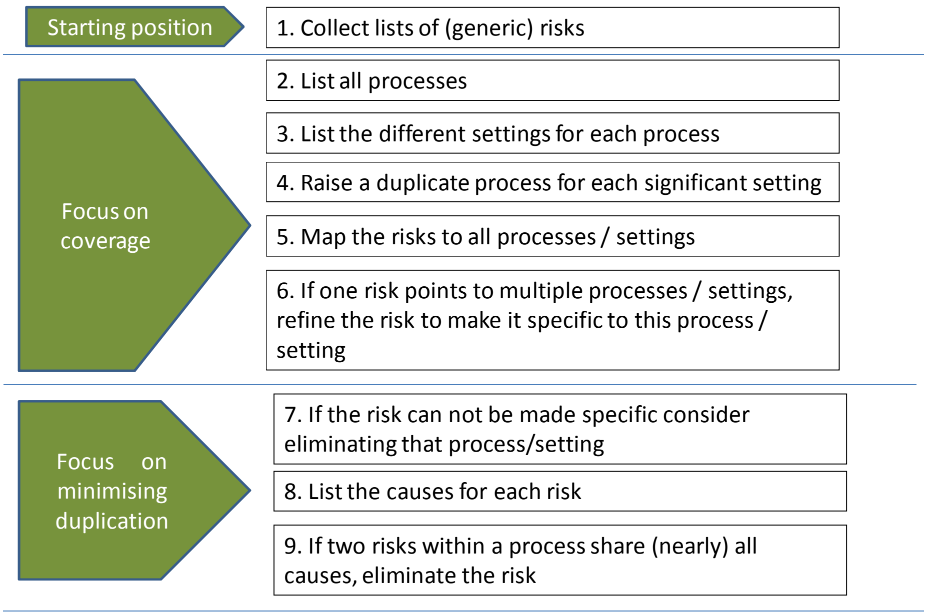
How to make it MECE

Making the library of risks MECE, we want to expand it where necessary, to reach comprehensive coverage. We also want to limit it where we can, to ensure mutual exclusivity. To do this, we take two big steps. First we expand the list of risks by recognizing that different processes in different settings lead to different risks. Next, we need to ensure that risks are specific. If we cannot make the risk specific to the process/setting, we have no need for it.

Finally, we examine the list for duplication by looking at the causes. Similar causes call for similar remedies, and hence from a risk management perspective, these risks are the same.

There are nine steps in the process, outlined in the diagram below:

Nine steps to making risks MECE



1. Collect lists of (generic) risks
To make our risks MECE, we need to have a starting point. Many banks use the Basel event categories as a starting point. To make sure that the risks in our library are not too broad, it is worthwhile to dig deeper than the first level (Internal Fraud, External Fraud, Clients Products & Business Practices etc) and to go to the third level or even the level of examples.

2. List all processes
All the bank's processes are prone to operational risk, and we should be specific about which risk is present in which process. Note that the level of detail of the processes needs to be reasonable. For our purpose of ensuring MECE risks for the bank, a rule of thumb is that a division, say retail or wholesale or asset management, will have more than 10, but typically significantly less than 100 identified processes, often not more than 50. Ideally, these should be mapped out, used and maintained, but not all banks manage the last two steps.

3. List the different settings for each process
Not all processes are implemented in exactly the same environment. Geographies, Legal environments, start up countries versus home countries etcetera, are environments that will impact the risk profile, Sometimes, the processes in these environments are captured under a single process description. For risk purposes, we want to differentiate between processes that are carried out in different settings *if the different setting can have consequences for the actual risk.*

4. Raise a duplicate process for each significant setting
Here, we need to make a clear judgment call. If the setting is such that it can be expected to alter the risk, then we raise a duplicate process for that setting. Thus, if "Account opening" has a

different risk profile in rural settings than in non-rural settings, we duplicate the "Account opening" process into "Account opening: Rural setting" and "Account opening: Non-rural setting".

5. Map the risks to all processes / settings

We map the risks from step 1 to the expanded process / setting list of step 4. Note that not all risks will be relevant to all process / setting combinations, so risks will not be distributed evenly. If the risks have the level of generality of the first level Basel II event categories, most risks are likely to be mapped to all process / settings combinations. The more specific the risks have been defined in step 1, the more sparse the mapping will be and differences emerge among the process / setting combinations.

6. If one risk points to multiple processes/settings, refine the risk to make it specific to this process/setting

To ensure that the risk description is meaningful to the process owners, and are not simply stating "Risk of Internal Fraud" we need to be specific about what kind of internal fraud we mean. So in the case of client account opening for rural branches, it could be: "The risk of willful misrepresentation upon account opening where the client has no passport or ID card but relies on referees".

7. If the risk cannot be made specific consider eliminating that process/setting

Sometimes, a risk cannot be made specific to a process / setting. If that is the case, it can suggest that this risk is actually not relevant here. If the risk is described at an abstract level (e.g. level 1) and cannot be made specific, we can delete it from the list.

8. List the causes for each risk

Now that we have a list of risks, we add the causes. Causes are prevailing circumstances that increase the probability of an event. By listing the causes, we define what are the underlying reasons this risk exists. It is important to be thorough and detailed in the cause listing. We start by asking "why does this risk exist?". Then for every answer, we again ask "why does this cause exist" until we have reached a granular level, and no further 'why' questions are meaningful.

9. If two risks within a process share (nearly) all causes, group the risk

Risks in the same process / setting with identical causes should be grouped under a single heading. If there is no difference in the causes, then there is no difference in the potential actions to take. The risks are better treated under one name and we can group the risks accordingly.
After these 9 steps, the list of risk should be both mutually exclusive (in the sense that they are specific and refer to defined processes / settings with unique sets of causes) as well as comprehensively exhaustive (in the sense that they cover all process / setting combinations).

Conclusion

Making risks MECE is expectations is a worthwhile exercise, eliminating double counting and still ensuring broad coverage. It is also no too hard if we follow the simple 9 step process.