GRAS Newsletter 59

June 2013

Circumstances Alter Cases

Summary: Major losses are the result of a host of circumstances and a chain of events. Analysing the risk drivers and understanding how events can cascade are thus basic requirements in OpRisk management. Many banks analyse events using the BIS event classification. The event typology, however, was designed to be a classification of *what* ultimately happened, not *how* it happened along the way. Thus, it fails to provide a full picture of all the risk drivers of an event. In this newsletter, we focus on a better way to classify underlying risk drivers. A sliding scale proves to be the answer.

Dear reader,

Managing tail risks requires out of the box thinking, especially regarding the circumstances that give rise to increased risk levels. Getting a grip on the prevailing circumstances (or risk drivers) requires thorough analysis and a framework that allows for a range of drivers. The Basel event categories, commonly used to classify losses, are not the best starting point for such a causal analysis. They were mainly designed to capture loss events, they were meant to be mutually exclusive, and to focus on the ultimate event. For causal analysis, we need to look at all aspects that lead to the event, not just the final outcome.

A sliding scale for the main classification

Since no single aspect can do justice to the complex of circumstances, we need a way to assess both the individual contribution of each circumstance as well as the combination with other circumstances. We do this by using a two tier table like the event classification, but with two important differences.

1. The drivers are not mutually exclusive. We implement this by rating each of the six main drivers rather than select only one.
2. All main drivers are rated on a scale, rather than on a yes/no basis.

The first table that needs to be filled in is given below. The ORM analyst is invited to score the *contribution* of each driver to the event. As an example: what may be classified as *Internal Fraud* in the Basel Event classification could be scored as follows for causal classification and analysis:

To what degree was the event driven by circumstances relating to:					
	Not at all	**Minimally**	**Considerably**	**Significantly**	**Predominantly**
1. Organisational set-up?			■		
2. IT Set up?	■				
3. Information Handling?				■	
4. Human Resources Issues?					■
5. Processing issues?		■			
6. External disruptions?	■				

Table 1. The first tier for identifying and classifying risk drivers

As new information comes to light, the weight of circumstances can change but we are unlikely to face the situations we sometimes encounter in event classification. Let us illustrate this: imagine a case of mispricing. Without other information, it might be categorised as *Execution Delivery –*

Process Management. When we find out it is a result of model failure, it could be re-classed as *Clients, Products and Business Practices*. Still later, when we discover that the model was developed by an external party to take advantage of a loophole to defraud the bank, it could become *External Fraud*. Finally, when we find out that our own staff I was complicit, it is again re-classified as *Internal Fraud*. For causal analysis this is not an issue since additional information does not change the classification, it simply enriches the knowledge base.[1]

A yes/no scale for the sub-classification

Once the contribution of each driver has been identified, we can examine the second level. Three rules apply here:

1. To make sure that only useful data is stored, sub-categorisation should only be done if there is sufficient information. If there is no information (yet), it should not be done at all.
2. Sub-categorisation does not require a sliding scale but a yes/no tick-box. Any driver that is selected inherits the rating of the main categorisation. This avoids spurious exactness.
3. It is good practice to fill in the sub-classification if the main rating is *Significantly* or *Predominantly*. For other classes, subdivision is not necessary.

In our example, *Information Handling* and *Human Resource Issues* should be further detailed. The second tier then looks could look like this:

Please tick one or more boxes indicating relevant risk drivers:	
3. INFORMATION HANDLING	
□	3.1 Inadequate handling of proprietary or confidential information
■	3.2 Inadequate control over integrity of information
□	3.3 Inadequate assessment of reliability of information
■	3.4 Inadequate control over availability of information
4. HUMAN RESOURCE ISSUES	
■	4.1 Poor integrity of staff
■	4.2 Failing recruitment
□	4.3Inadequate development of staff competencies (knowledge and skills)
□	4.4 Insufficient attention for staff health and safety
□	4.4 Key man exposure

Table 2. The second tier for identifying and classifying risk drivers

Conclusion

When we analyse risk drivers, we must find a simple way to identify multiple circumstances. Once a risk driver has been chosen, the second tier only needs to differentiate between *aspects* of that cause. Using this classification will help identify which circumstances gave rise to the event, rather than only indicate what happened as a result of these problems.

[1] Note that this approach automatically takes care of the perennial discussion of identifying the "root" cause. One interpretation of 'root cause' would be the driver with the highest rating, which can of course be more than one. Some banks have taken the approach that "root" cause is simply the first moment of failure. A more useful approach is to follow a full root cause analysis. That means examining the whole sequence of events. Any element within the timeline can be part of the crucial set of circumstances which lead to the loss event, not just the first one identified. See newsletter 9 on Fault Tree Analysis: http://www.globalras.com/Topics/GRAS%20Nr%209%20Fault%20Tree%20Analysis.pdf

Appendix I: Drivers of OpRisk

	Drivers of OpRisk:		**Subdivided into:**
1	ORGANISATIONAL SET UP	1.1	Inadequate segregation of functions
		1.2	Unclear responsibilities
		1.3	Inappropriate responsibilities
		1.4	Inadequate internal governance structure
		1.5	Poor quality of management
		1.6	Other inadequacies in organisational set up
2	IT SET UP	2.1	Inadequate IT strategy
		2.2	Inadequate IT-policies
		2.3	Inadequate IT-standards
		2.4	Inadequate IT solution delivery
		2.5	Inadequate IT support
3	INFORMATION HANDLING	3.1	Inadequate handling of proprietary or confidential information
		3.2	Inadequate control over integrity of information
		3.3	Inadequate assessment of reliability of information
		3.4	Inadequate control over availability of information
4	HUMAN RESOURCES ISSUES	4.1	Poor integrity of staff
		4.2	Failing recruitment
		4.3	Inadequate development of staff competencies (knowledge and skills)
		4.4	Insufficient attention for staff health and safety
		4.5	Key man exposure
5	PROCESSING ISSUES	5.1	Ill designed processes
		5.2	Inadequate procedures
		5.3	Poor adherence to procedures
		5.4	Poor monitoring of adherence to procedures
		5.5	Inappropriate models
		5.6	Inappropriate dependency on external suppliers/staff
6	EXTERNAL DISRUPTION	6.1	Natural disasters of an unanticipated scale
		6.2	Other accidental of an unanticipated scale
		6.3	Changes in the social, legal, or political environment of unanticipated scale
		6.4	Business disruption of an unanticipated scale
		6.5	Uncontrollable criminal attacks

Table 3. Drivers of Operational Risk