Operational (R)isks and their (R)oots, (R)esults and (R)emedies

By: Greg Suddards

A number of discussion topics on various Linked-In groups in recent months have suggested that the four issues above warrant serious consideration. Rather than devote attention to the question of which is involved in any particular debate, the tendency, it would seem, has been for practitioners to define new categories of risks. Inevitably, the risk universe has been expanded rapidly but the consequence has been confusion. The thoughts below on the subjects, therefore, have been posted in the hope that they will encourage sufficient discussion to bring clarity to the various concepts. After all, if practitioners cannot gain consensus it is difficult to imagine how risk managers will earn credibility with management. The comments in the remainder of the article are confined to Operational Risk Management where the least cohesion appears to exist although they ought to have just as much relevance to the disciplines of Credit Risk, Market Risk, Liquidity Risk, Margin Risk and Strategic Risk.

The Basel Committee defined Operational Risk as the risk of loss from failed or inadequate people, process and systems or from external events. It includes Legal Risks but excludes *so-called* Strategic and Reputational risks (italics added). Perhaps a great many of the difficulties encountered by practitioners in the field of Operational Risk Management (ORM) derive from this definition. The definition makes no reference to the types of risks contemplated under the banner of Operational Risks. Rather, it is a typology, of sorts, of the (R)oot causes of risks in general. And herein lies the rub. An external event, for example, would include the onset of economic recession and undoubtedly this may result in various operational risk events (for example, internal fraud due to declining household incomes) but it also has everything to do with loan defaults (Credit Risk) and adverse asset price movements (Market Risk). Consequently, a definition which is based on (R)oots (or, causes, or drivers) is unsuitable.

It is trite that Operational Risks must have to do with the operations aspects of an organization. Following Porter (Competitive Advantage, 1985) each functional area, not just the Operations function, has its own production function or *modus operandi*; that is to say, it deploys resources and procedures to achieve its objectives effectively and efficiently. Conversely, anything which prompts failure to achieve the objectives efficiently and effectively must constitute an Operational Risk. Consequently, it is possibly more accurate to consider Operational Risk as the risk of loss from inefficient or ineffective deployment of resources and or procedures whether induced internally or externally. This would render resources and procedures germane to any event of an Operational risk nature; in other words, if neither of these facets is impacted, it is unlikely that an event of Operational Risk

has occurred. On this basis there is little doubt that other types of risk are excluded from consideration from the criterion.

Contrary to its definition of Operational Risks, the taxonomy of events contemplated by the Basel Committee is comprehensive, having been defined down to third level of detail. High level tests performed by the author against industries outside of financial services indicate that they cater for virtually all event-types of an Operational Risk nature. Importantly, the reasoning in the previous paragraph is consistent with this taxonomy. This is demonstrated below in respect of each of the broad (high level) categories identified by the Committee, namely:

Internal and External Fraud (connoting more resources have to be deployed than are necessary);

Damage to Physical Assets (requiring non-productive expenditure to either repair or replace assets);

Business Disruption and System Failure (necessitating suboptimal "work-around" procedures);

People Practices and Workplace Safety (which cause fines, or damages claims and, hence, expenditure in excess of what is required for efficiency);

Clients, Products and Business Practices (which imply that resources and/or procedures have not been applied efficiently or effectively); and,

Execution, Delivery and Process Management Shortcomings (which also refers to poor application of resources and procedures).

This introduces the first of the discussion topics which has done the rounds at least once, namely, whether Compliance Risk is an aspect of Operational Risk or a separate category. As alluded to earlier, every functional area of an organization has its own *modus operandi* for achieving its objectives whether these are committed to writing or not. These define what has to be done, by whom and when and they invariably determine output quotas and quality standards which have to be complied with. Obviously, the task of managing this resides with line management. On occasion, these procedures and the resources to be deployed are modified by legislation. The question, therefore, is whether compliance with procedures determined without reference to legislation (but in terms of organizational standards) and those modified by the intervention of regulation, should be managed and overseen by different sets of people and the answer is "no". Indeed, many of the Operational Risk categories have large legal compliance components (*vide* Employment Practices, Clients etc, and Execution etc). Surely, compliance is compliance whether induced by regulation or not. Non-compliance with regulatory requirements invariably culminates in fines or forfeitures which connote deployment of unnecessarily large quantities of working

capital to the process or procedure concerned. Consequently, one is lead to the conclusion that Compliance is an element of Operational Risk and is not a risk category in its own right. Obviously, the Operational Risk function might include a person(s) skilled in regulatory compliance to assist it in its tasks.

If an earthquake were to occur without impacting on either the resources or the procedures of an organization it is concluded that an event of an Operational Risk has not been experienced. One cannot then speak of the *risk of an earthquake* despite the very real threat of its occurrence. The risk, as mentioned previously, is that the efficiency or effectiveness of a function is adversely affected and, of necessity, that must entail resort to a suboptimal procedure or excessive expenditure on resources. Although the earthquake is not a risk it is certainly an event of which the risk manger needs to be cogniscent in order to understand the risks to which the organization is exposed. The earthquake is a (R)oot cause or hazard or driver of the Operational Risk. It is an example of an external inducer of risk. Other examples of external drivers would be hail, floods, fires emanating from outside the organization and, public transport disruptions. Examples of internal drivers would be inadequately skilled employees or dangerous procedures or unstable systems. This is the sense in which the Basel Committee related people, processes and systems to Operational Risks.

It is important in the context of managing Operational Risks to commence at the level of a procedure or at most at the level of a process. For, which drivers are internal and which are external, is depends crucially on the sequence of procedures. When one procedure is dependent upon the output of another for its inputs what is a (R)isk to the upstream procedure is a (R)oot cause to its downstream counterpart. Within the context of a mortgage division in a bank, for example, the information system is a resource which it employs along with its employees and premises. The mortgage division does not own the information system and, consequently, it would not suffer loss from damage thereto unless its own employees were responsible for the damage. The risk which the mortgage division perceives if the system were to fail for any reason is business disruption – it will be unable to process mortgage applications or recover from its debtors. Apart from itself being remiss in failing to ensure that its employees are adequately skilled to use the system, it looks to the competence and reliability of its vendor, the bank's own IT department, as the driver of the risk; it is unconcerned with the details of what happens on "the other side of the wall". In the IT department, however, its output (systems availability) is dependent on the integrity and availability of its hardware and software, power supply and the skills which it employs and it will suffer loss immediately if these are damaged or destroyed because it owns the resources concerned. That is to say, its risk is Systems Failure. An earthquake which could potentially destroy the computer centre is a significant hazard or driver of its risk.

At the level of an organization one would have to perform a consolidation of sorts setting off risks in one department against drivers in downstream procedures and processes. In the example above this would be conducted as follows:

IT Dept: Earthquake (Root) → System Failure (Risk)

Mortgage Div: System Failure (Root) → Business Disrupt (Risk)

Organization: Earthquake (Root) → Business Disruption (Risk)

It is the experience of the writer that this methodology is crucial to avoid confusion.

This leads naturally into the next discussion topic on Linked-In, namely the confusion of (R)isks with (R)esults. The extent of the loss incurred in consequence of the (R)isk event is the (R)esult or severity of the event (or Loss Given the Event) but it is not a risk *per se*. All risk managers would be clear on this but in practical applications the distinction is not always obvious. In one discussion topic an organization had suffered loos as a result of spillage of dangerous chemicals from a neighbouring manufacturing concern. The question raised was how ought the affected organization to categorise the risk that it may be unsuccessful in its claim for compensation from the offending organization. Analysis of the case suggested that the correct event category was *Damage to Physical Assets* to record the loss of inventory, injuries to employees and damage to plant and equipment. The (R)esult of the event was the monetary value of compensation to employees, damages and write offs as well costs incurred in the claim for compensation less the likely amount recoverable from the offending organization.

But, what if no financial loss is immediately apparent? One is reminded of the case of the large U.K. clearing bank which had adopted the procedure of sending by overnight mail to its off-site storage, back-up disks containing customer information until, one night, when the disks went missing (Fitch, New Losses, Algo Newsletter). Apparently, customers were not prejudiced by the event and the bank suffered no losses. It is possible, however, that some customers may have been induced to move their relationships to competitors, others may have declined to increase their relationships through new products and still others may allowed the bank one “last chance” before moving their banking accounts to a competitor and, many would no longer recommend the bank to friends. That is to say, the bank possibly experienced severe reputational damage as a result of the Execution, Delivery and Process Management event (the poor procedure for transporting the back-up disks). This makes adverse consequences for an organization’s reputation a (R)esult, not a (R)isk. There is no case for the so-called category of Reputational Risk.

The final point concerns the confusion of (R)emedies (otherwise referred to as controls and mitigants) with the (R)isks themselves. The discussion which prompted the comments below concerned the appropriate reporting line foe Business Continuity; in particular, the issue was whether business continuity is a separate risk category warranting direct responsibility

to the Chief Risk Officer or whether it ought to report through Operational Risk Management. Again the first reaction apparently had been to define a new category of risk, namely Business Continuity Risk. This is in itself is a contradiction – the risk must surely be Business Discontinuity. Immediately that the problem is cast in these terms, however, the answer becomes obvious. Business Discontinuity is identical to Business Disruption which is an established category of Operational Risks in the Basel taxonomy. A Business Continuity Plan is simply a mitigant to protect an organization against the risk of Business Disruption.

Conclusion

From various discussion topics posted on Linked-In the tendency seems to be that practitioners in the field of Operational Risk Management are too eager to cry "Separate Risk Category" rather than think carefully through the events. The Basel taxonomy of Operational Risks, however, is sufficiently robust to accommodate virtually all situations. Hence, as a first step it is good practice to write down all the facts surrounding each event. Anything which takes place after the appropriate Basel (R)isk event category is first likely to be a (R)esult or severity and then a (R)emedy. The most difficult step in the process is to separate (R)isks from their (R)oots because (R)isk events from upstream procedures or processes become (R)oot causes to their downstream counterparts. Consequently, each process (or preferably, procedure) ought to be clearly circumscribed in terms of what its management can control. Of necessity, the methodology in all of the above has to be carefully thought through.