How to Categorize Operational Losses?

Applying Principles as Opposed to Rules

Background

My concerns with the current categorization system are based on my own personal observations of the way in which our clients and members of my own team were interpreting the BIS classification standards while categorizing both internal loss data and external public loss data. These problems became apparent to the entire team in early February of this year at the conclusion of a major clean-up exercise involving our external public loss database. The goal of this effort was to ensure our application of the BIS standards was logical and consistent. Instead, following this exercise, there was a clear consensus among the team that this objective was not being met and that there was something clearly wrong with the existing BIS classification structure.

Summary of the Problem

The BIS framework is designed to be an "Event" based approach. There are seven event categories at the primary level. Unfortunately, two of these categories—Clients, Products and Business Practices (CPBP) and Execution, Delivery and Process Management (EDPM)—are defined as mixtures of causes and events, whereas Business Disruption and System Failures (BDSF), another primary category, is defined as a mixture of causes, events and effects. Damage to Physical Assets (DPA), another primary category, is both an event and an effect. Unauthorized Activities (UA), which is defined as a secondary category under Internal Fraud (IF), actually includes certain non-fraud (negligence-related) events that are very similar to those included in CPBP. Some other IF activities also more naturally belong in CPBP, or both in IF and CPBP. And to further compound the problem, there are certain CPBP events that belong more naturally in IF, or in both CPBP and IF.

Categorizing in this manner is like categorizing by shape—using squares, circles, triangles and rectangles—while simultaneously categorizing by color—identifying some objects as red, others as blue—and then making an exception, for example, by moving all rectangles of perimeter 16 in the square category, since 16 is equal to four squared.

As you can see, the problem with the BIS structure is that it is logically inconsistent and contains overlapping identifications, and hence is conceptually flawed. For example, CPBP is defined as "losses arising from an unintentional or negligent failure to meet a professional obligation…" It is easy to see that this category is

therefore defined in terms of a cause, which spans multiple events, and is potentially correlated with other categories, such as EDPM and IF, which may also contain the same types of events. What's more, because CPBP is defined in terms of negligence, it is possible that a set of rules that (directly or indirectly) includes negligence in its standards is likely to contain a disproportionate number of the larger overlapping losses. This will cause significant problems in modeling.

Given this potential for overlaps, it is clear that we need to have rules for determining how to draw lines between two types of categories. These rules should be logical and easy to understand and apply, and they should not violate any modeling principles. An approach that attempts to come up with a set of rules to ensure consistent categorization alone is not sufficient.

The fact that we haven't yet come up with an efficient system for categorizing loss events may be attributed to our limited understanding of the problem. Before one can solve this problem one must first get to the root cause, otherwise we will be continuously finding stopgap or band-aid solutions to what are actually just symptoms of the real problem. What we need is a clear set of rules to determine how to differentiate between any two types of events and how to deal logically and consistently with the overlaps. First let us define our goal as an approach that optimizes categorization based on the following considerations:

1. *Management Information:* The categories should be defined in a way that makes the information useful for management purposes. The definitions should ensure homogeneity of risk types. Failing to address this problem limits the use this information can be put to.

2. *Logical consistency:* The definition of the category at the highest level should be perfectly consistent with the examples at the lowest level. The types of events in the second tier should be perfect subsets of the event in the first tier, and so on. One should be able to go from left to right and right to left without any inconsistencies. There should be no redundancies. A term should only be used once. Failing to address this problem will cause confusion in usage.

3. *Statistical purity:* The underlying data sets should not be correlated, and at the lowest level should represent homogenous distributions[1]. Failing to address this problem will result in the generation of potentially misleading information.

[1] Mixing two non-homogenous data sets into a single distribution may make modeling the resulting distribution a very challenging technical problem. In addition, the resulting VaR figures may be difficult to interpret for management purposes. (Consider the technical problems associated with modeling the risk from both hangnails and hurricanes through a single severity distribution. And what would be the value of this information?)

A Solution

I start with the fundamental belief that the *true* solution to this problem will be elegant: you know you have gotten it right when your solution is clean, unambiguous and (borrowing a cliché from the discoverers of the structure of the DNA molecule) *"beautiful."*

Let us begin by addressing the overlap between Internal Fraud and CPBP, though not by comparing activities, but instead by examining conditions. First of all, we need to ask ourselves, What are we trying to capture in these two categories? It appears that we want to differentiate between events that really are crime-related and those in which people simply "skirted the law" or were aggressive in following a guideline or policy. However, when examining activities, it becomes apparent that many CPBP categories are based on the results of intentional criminal acts (e.g., insider trading, antitrust and money laundering). The only thing unintentional about such events is that the offending party did not intend to get caught – a goal that is the same for criminal acts.

This traditional approach to CPBP introduces potential for confusion and could result in inconsistent categorization and/or mixing of correlated distributions.

So what's the real difference between Fraud and CPBP? Suppose we say that CPBP events are those in which a person did not steal from the firm, but was a firm employee, who intentionally committed a crime that was intended to benefit the firm (and eventually himself, either through bonuses, promotions, or the avoidance of termination). This makes conceptual sense, because it is consistent with the events we want to include in CPBP. Unfortunately it also includes unauthorized activities, which BIS puts into Internal Fraud, but perhaps we should put this matter aside for the time being.

Continuing along this line of reasoning let us view this issue the way someone in the field of decision sciences would apply game theory, by looking at the potential outcomes to all involved parties through a "payoff matrix."

Let us consider two questions/criteria for the proposed payoff matrix:

1. Who benefits (or who was intended to benefit)?
2. Who loses (or who was intended to have lost directly or economically)?

For who benefits, there are four possible answers: the Individual, the Firm, a Counterparty and No one. For who suffers a loss, there are again the same four possibilities.

Fraud

Because we believe all criminal acts must involve an intent to benefit the perpetrator, let us establish this as one criterion. (Benefit, in this context, includes anything that increases utility, and should not be narrowly construed in only pecuniary terms.) Criminal acts also involve some sort of zero sum game (i.e., for each winner there needs to be a loser). Putting this information together we can create a payoff matrix for Internal Fraud.

The following two tables define the category Internal Fraud:

FRAUD		Intended Beneficiary			
		Individual	Firm	Counterparty	No one
Intended Loss Sufferer	Individual				
	Firm	X			
	Counterparty				
	No one				

FRAUD		Intended Beneficiary			
		Individual	Firm	Counterparty	No one
Intended Loss Sufferer	Individual				
	Firm				
	Counterparty	X			
	No one				

In other words Internal Fraud is defined as an act in which:

1. The individual(s) perpetrating the act is the intended beneficiary; and
2. Either the firm or one of the firm's counterparties is expected to suffer a loss.

These conditions line up very neatly with our conceptual understanding of internal fraud. For example, they encompass fraud, credit fraud, theft, extortion, embezzlement, robbery, misappropriation of assets, forgery, check kiting, smuggling, account takeover/impersonation and insider trading on the individual's account, all of which are on the BIS list.

This set also includes the well-known Joseph Jett event, in which the accused was found not guilty of fraud. (One convenient property of this standard is that it is not impacted by the legal system).

Interestingly, this set does not include: tax non-compliance/evasion (willful) when committed by an employee on behalf of the firm, and bribes and kickbacks that do not involve extortion, even though these issues are currently included in the BIS list of Fraud events. This highlights a logical inconsistency, which should be remedied through respecification. I believe that these event types more logically belong in CPBP.

Fraud may or may not include malicious destruction of assets, depending on how one wants to deal with the overlap with damage to physical assets.

Note: I would recommend that we separately classify losses to the firm and losses to a counterparty, because we may later determine that the distributional characteristics differ, and furthermore there may be important managerial/control reasons for separating these two sets.

CPBP

Let us now attempt to do the same for CPBP. Let us define CPBP as all types of illegal, quasi-legal and questionable events committed by a firm employee, where the individual is intending to benefit the firm (and eventually himself directly or indirectly) at the expense of some other party. And all types of similar events where there may not be a loser (i.e., the counterparty also gains), for example exceeding client exposure limits. Putting this information together we can create a payoff matrix for CPBP.

The following two tables define the category CPBP:

CPBP		Intended Beneficiary			
		Individual	Firm	Counterparty	No one
Intended Loss Sufferer	Individual				
	Firm				
	Counterparty	X	X		
	No one				

CPBP		Intended Beneficiary			
		Individual	Firm	Counterparty	No one
Intended Loss Sufferer	Individual				
	Firm				
	Counterparty				
	No one	X	X	X	

In other words, CPBP is defined as an event in which:

1. Both the individual and the firm were intended to benefit, and a counterparty (which could include a government) was expected to incur a loss; or
2. The individual, the firm and the counterparty were all intended to benefit, and no one was expected to incur a loss.

These standards line up very neatly with our conceptual understanding of CPBP, which would include suitability breaches/guideline violations; suitability/disclosure (KYC, etc.) issues, retail consumer disclosure violations, breach of privacy (where it benefits the firm), aggressive sales, account churning, misuse of confidential information (where it benefits the firm), lender liability (where the loan was given in the interest of the firm), antitrust, improper trade and market practice, market manipulation, insider trading, unlicensed activity, money laundering, failure to investigate client per guidelines, exceeding client exposure limits, and disputes over performance of advisory activities.

This category also includes unauthorized activities (which the BIS places under Internal Fraud) a pairing that is logically consistent, since unauthorized activities are generally activities in which the firm is not intended to be a loser.

This category also includes penalties from bribes/kickbacks (bribes and kickback payments should not be included as operational losses; unless considered extortion, they are expected costs), willful non-compliance/tax evasion, and insider trading.

The only things from the BIS list this category does not include are product defects and model errors, which I believe more naturally fall into EDPM.

Note: in all CPBP events, the firm is not intended to lose, but loses only because things did not work out as planned.

EDPM

Now lets consider EDPM. The original theme of EDPM was accidental errors. How should we characterize this risk category in the context of game theory? It would appear an EDPM event is one in which the transaction is in the process phase. At this point there is no opportunity for additional gain, and the intention is not to cause anyone a loss. Thus, one can construct a payoff matrix for EDPM as follows:

The following table defines the category EDPM.

EDPM		Intended Beneficiary			
		Individual	Firm	Counterparty	No one
Intended Loss Sufferer	Individual				
	Firm				
	Counterparty				
	No one				X

Therefore EDPM is defined as an event in which there was no intended beneficiary and no intended loss sufferer.

The current BIS list of EDPM events lines up perfectly with this structure. This includes: miscommunication, data entry, maintenance or loading error, etc.

Conclusion

I think the main problems with the current BIS categorization system is that the primary level categories are described in words that are confusing and misleading. There are also some inconsistencies in the structure. Nevertheless, the foundation upon which this structure is based is generally sound.

What has really been lacking is a clear way of describing the top-level risk categories in abstract terms rather than through a set of complicated rules.

In this paper I have presented an approach, which I believe elegantly addresses this problem. It also helps highlight the small number of inconsistencies in the current approach, where certain low level risk types were inappropriately placed in the wrong risk category (based on their homogenous risk characteristics).

In summary, by applying conditions, not rules, we can define certain risk categories as follows:

Fraud (internal or external) is an event in which:

- The individual(s) perpetrating the act is the intended beneficiary; and
- Either the firm or one of the firm's counterparties is expected to suffer a loss.

CPBP is an event in which:

- Both the individual and the firm were intended to benefit, and a counterparty (which could include a government) was expected to incur a loss; or

- The individual, the firm and the counterparty were all intended to benefit, and no one was expected to incur a loss.

EDPM is an event in which:

- There was no intended beneficiary and no intended loss sufferer.

These rules are unambiguous, are logically consistent, do not violate any modeling principles and should be very easy to apply in practice. This same approach we applied above to Internal and External Fraud, CPBP and EDPM should also be applicable to the other risk categories. I would also like to use this framework to address the more challenging and pertinent issue of determining how to differentiate loss event categories at the next level, preferably establishing a level where there are between eight and twelve risk categories

* * *