Data Governance and Operational Risk: Issues and Questions for a Research Program

Vasant Dhar
Professor and Director
Center for Digital Economy Research
Stern School of Business
New York University

This document summarizes key issues and questions related to data governance and operational risk. It is based on panel discussions at the CeDER workshop on October 31, 2006 and summaries of follow-up discussions with some of the panelists. Its purpose is to initiate a public discussion of the major issues and questions involved in data governance and operational risk.

1. Facts
Operational risk continues to grow in size due to business expansion, new products, and greater dependence of complex processes and systems.

We know what the distribution of losses look like. There are lots of events of low severity and a few of high severity. For the more frequently occurring ones, faults can be identified to explain loss patterns.

Joe Sabatini of JPMorgan Chase underscored the need to understand loss patterns. ORX, for example, is creating a database of anonymized loss patterns from member data. At the very least, this data will have forensic value. Understanding where and why losses are occurring will make it meaningful to ask if these patterns of loss could occur in other business units or activities. This will also allow benchmarking business units against each other and against peer banks to measure and provide incentives for better performance.

However, the hard knocks come from a few, very low frequency events of high severity (LFHS) that can be devastating. These events need to be anticipated and actions taken to avoid them. They also need to be priced so that the appropriate amount of capital can be allocated to cover them when they do occur. Or, whenever possible, some risks can be offloaded in a commercially viable manner.

2. Research Questions
There are several research questions related to operational risk. (These are boldfaced in the text that follows.) One interesting question, given the importance of the high severity events, is:

Is there a “signature” to low frequency high severity (LFHS) events?

It is not clear whether the answer to this is a yes, and if so, what such a signature would look like. What we’d like to know is whether there is a predictive model that would indicate the probability of an LFHS event occurring in an organization.
Sabatini pointed out that data from areas such as aviation show that major losses do not result from a single point of failure. What this suggests is that several things conspire to go wrong at once and slip through multiple checks. When the series of checks is only as strong as its weakest link, it becomes important to identify the weakest link. However, the series of checks are often not independent, in which case one failure may increase the chances of others occurring. In other words, a sequence of certain failures may be indicative of a higher chance of major losses in the future.

Judson argued that once a major loss occurs, actions are generally taken to fix systems and/or processes so that an identical (or similar) loss does not recur. This implies that the predictive value of past data is limited for future LFHS events, especially in the same business unit.

What data, other than past loss patterns, might be useful in estimating the probability of an LFHS event, i.e. $p(\text{LFHS})$? One variable is the “risk culture” of an organization. One would expect that the quality of a unit’s internal controls, which includes the extent to which it emphasizes a risk-oriented view to business, would lower $p(\text{LFHS})$. The nature of incentive systems in an organization are also indicative of risk culture, although this becomes hard to measure. Nevertheless, the question this raises is: what is the best way to create and measure the required risk culture to prevent LFHS?

Marcelo Cruz suggested that regression models can be constructed that provide some predictive value for loss events. What would be the independent variables in such a regression model? Past losses? Culture? Does this approach apply more for losses that occur more frequently and are of lower severity? In general, there is need to take data analysis to a new level of sophistication where we can link loss patterns and control measures to business or risk culture. It also makes sense to understand how risk and loss patterns evolve through a full product life cycle. It is the case that operational risk correlates with credit risk and market risk at earlier stages of the product life cycle, but less so at later stages?

Finally, there is a need to develop cost effective and credible capital measures for operational risk and to link these to product pricing, budgeting, business performance measures and compensation schemes. This will provide a foundation for improving financial performance through a better understanding and measurement of operational risk.

Mike Stiglianese made several observations. First, that information technology increases productivity, but often at the expense of security. Giving people more flexibility and tools to be productive also exposes an organization to unforeseen risks, as several high profile incidents have revealed over the last year.

Stiglianese focused mainly on information security. He pointed to the need to consider reputation risk as part of security policy, and that considering reputation risk may lead to policies or processes that are different than those that might result from a consideration of inherent risk alone. It is necessary to factor reputation or other 'soft' risks into operational risk management processes other than probability of occurrence and severity. Reputation risks are very real and can be
quite painful even if they are not directly linked to financial losses or are otherwise hard to quantify. Where quantification is difficult, many firms have chosen to employ some version of the Risk/Probability /Impact template similar to that presented by Mike. This is a helpful way of prioritizing non-quantifiable or low frequency risks.

Moss focused on the need for self assessments of risk, and suggested steps to increase the effectiveness of self assessment in organizations. The issue of self-assessment was also discussed briefly by Sabatini. While SA is important, more does not mean better. What this suggests is that SA is likely to be much more effective if it is conducted in an environment where the risk culture is strong.