RISKY Business!

Using Business Intelligence to Mitigate Operational Risk

By Claudia Imhoff

There have been several articles expressing a lot of interest and concern recently about operational risk (OR) and what it means to your organization. However, most of the articles deal with the mechanics of OR, instead of with how to mitigate or even eliminate it. Thus, it's time we take a long hard look at OR and understand that business intelligence (BI) is your best mechanism to reduce overall risk to the corporation's operations.

First, let's start with a basic definition of OR so we're all on the same page. According to the Office of the Comptroller of the Currency (OCC), OR is the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events.[1] It includes failure to comply with laws (legal risk) and the failure to comply with prudent ethical standards and contractual obligations. The well-documented examples of OR are:

- Internal fraud: act intended to defraud, misappropriate properties or circumvent regulations involving at least one employee.
- External fraud: same as internal fraud but involving a third party.
- Employment practices and workplace safety: act inconsistent with employment, includes injury claims payments and diversity/discrimination.
- Clients, products and business practices: unintentional or negligent failure to meet obligation to specific clients or resulting from product design.
- Execution, delivery and process management: failed transaction processing or process management from relations with trade counterparties or vendors.

According to the OCC, risks can stem from people, processes, technology and even external events. In the case of people, it means a risk of management failure, organizational structure or other HR failures. For processes, it consists of breakdowns in established procedures, the failure to follow these processes or inadequate process mapping (interfaces) between business units or lines of business (this includes IT as well). OR is also found in your technological environment. Here, it is both disruption and outright technology failures in internal as well as outsourced operations. The last source of OR is from external events such as natural disasters, terrorism and vandalism. These are obviously much more difficult to predict but are also much less common. As you can probably imagine, OR is not confined to any particular line of business, product type or organizational unit.

Unfortunately, just as OR is heating up, we find that its governance is still quite immature. Many organizations are unsure of exactly how to administer a ruling body responsible for OR. This is where BI comes in. How does BI help? First, let's look at BI's main purposes and then how we can use it to mitigate OR. BI serves two main purposes:

- It monitors the financial and operational health of the organization. This is the rearview mirror look at the enterprise. It shows what has happened in recent history, a traditional role for BI. Many organizations use these lagging indicators to spot trends or patterns in historical events. For example, they are useful in studying fraudulent behavior.

- It regulates operations of the organization through alerts, alarms, key performance indicators (KPIs) and dashboards derived from analyzing operational streams of data. Leading indicators from predictive analytics or guided decision-making capabilities are used to adjust the enterprise should something go off-kilter. It is through these leading indicators that BI contributes the most to proactively managing OR.

OR management must be able to differentiate high-frequency, low-impact (HFLI) events from low-frequency, high-impact (LFHI) events. HFLI events include such things as minor accounting errors and bank teller mistakes. These happen frequently but are not considered significant in terms of the OR of the enterprise. They may be annoying, but they are not devastating to the overall health of the company – unless there is a pattern to the behavior.

LFHI events are the ones you want to catch quickly. These include major fraudulent activities and patterns of financial abuse. These are the types of events that brought down Enron, WorldCom and HealthSouth. Fortunately, their frequency is low because they cause significant – even fatal – damage to the company.

The difficulty is in differentiating between the two types of events. To differentiate between an exception (small, minor accounting errors) and a pattern of corruption (money-laundering), you must have high-quality, detailed data available. Unfortunately for many organizations, their BI environments consist of only OLAP or multidimensional capabilities. While good at identifying gross trends or patterns, these aggregations, averages and/or derived pieces of data can actually mask what is really happening. Traditional approaches can oversimplify or hide significant data points. Even the use of linear regression techniques can be misapplied or give misleading directions.

To manage OR, you must have massive amounts of *trustworthy* data and an architecture, such as the Corporate Information Factory (CIF), to map out the storage and usage of data. A BI architecture

clearly demonstrates the data flows into/out of various BI components and their process interactions. It establishes information as a corporate asset and promotes the seamless integration mandatory for better quality data. The architecture also enables reuse of the components, thereby reducing development costs and ensuring a coordinated deployment of business performance management (BPM), business activity monitoring (BAM) and other BI technologies for managing OR.

While certainly an obligatory part of any corporation's drive to mitigate OR, the CIF alone is not sufficient. You must have advanced analytical capabilities and the detailed data to support them. Perhaps your best advisors to determine appropriate analytics and causal models are the risk managers themselves. You can then begin to create an extended enterprise business analytics and metrics system to be used by analysts, managers and executives alike. To do so, you can leverage enabling technologies and architecture for risk measurement, financial metrics and predictions. These will require access to different types of data (behavioral, financial, demographic, etc.) and the development of linkage models that produce the "metrics that matter" for C-level executives, division and unit managers – ultimately for all knowledge-workers.

The techniques for analyzing, predicting and ultimately preventing OR go from simple to complex, from "estimates" to more precise metrics. For example, the model for HFLI events will have a completely different distribution than that for LFHI events. Employees may need to be trained or retrained on how to interpret these distributions. My advice is for your company to expand on its existing OR methodology to identify what could go wrong, come up with possible scenarios, perform proper analytics (causal models, etc.) to determine likely outcomes of both types of events and finally determine the actions to take for all events. However, it should be noted that businesspeople may be skeptical about converting "their judgment" into a statistical model. You may need to educate these people regarding BI and its capabilities as well as gain their confidence that your environment has good data, produces reliable numbers and has consistency across the enterprise. Their buy-in increases as more events are predicted and experienced – from credit defaults to natural disasters.

How do you get started? Here is a list of eight actions to get you going down the path of better OR management:

1. Start with basic definitions of OR. It is essential that you develop a common language for OR and its measurements across the enterprise. Part of the taxonomy should be how you define, calculate and categorize operational losses and what is meant by exposure and risk.
2. Develop detailed plans for controls on basic financial systems. You will also need to create a steering committee of top execs to ensure cooperation and acceptance across the enterprise.
3. Create a technological infrastructure, based on a proven architecture, to facilitate the use and integration of data from different systems. You may choose to create a center of excellence for data integration and another center of excellence for analytics. From these, you can begin to create appropriate analytics (e.g., predictive and guided decision-making capabilities) and to gather, store and make accessible the meta data behind the data.
4. Look for places where data integrity/quality can slip through the cracks. In particular, watch out for "customizations" to key systems. Ensure that your key operational systems have adequate audit trails for both the collection of the data and the processes behind the collection.
5. Standardize your technological aspects where possible. This standardization includes operational systems, BI components and all infrastructure components. It may be that the day of the "best of breed" contests is over.
6. Set up systems to automatically notify key constituents (senior execs, board members, accountants) of potential or real OR events. The use of BAM or BPM technologies in conjunction with traditional BI components overlaid with portal technology will greatly enhance your overall OR mitigation.
7. Intertwine IT projects with accounting processes to ensure clear identification of OR aspects. Where is an OR event likely to happen? Focus on the key measurements, normal ranges and thresholds surrounding that event. Develop appropriate KPIs or metrics based on this input and make sure that processes and procedures are fully documented and socialized. Understand how policies and procedures will be enforced. These may require the establishment of regular internal audits and checks.
8. Finally, don't forget about the cultural/organizational changes that must occur throughout the enterprise. All employees must be educated about their role in OR mitigation – how to determine an OR event, who to report it to and what actions to take. Make sure that they have access to BI applications that monitor exposure areas and detect losses. These are not simple reporting applications; they contain highly complicated and complex models. Therefore, employees must be educated on how to interpret the results from these models and data being generated.

Direct Your Focus

Operational risk, along with legislated compliance, is causing massive overhauls of most large organizations today. Unfortunately, we are still unsure of the actual requirements behind both of these mandates. This insecurity still appears to be the biggest hurdle for most enterprises. Certainly, reacting today while the actual rules are still unclear may leave companies playing catch-up in future. You would be wise to direct your company to focus on the visibility of its data, accountability of its employees and better governance over its technical aspects. IT plays a significant role in each of these aspects.

As a last thought, it must be realized that data integration is the driving force behind any sound OR management function. Without a doubt, it is the best time to create a world-class integrated environment. Use OR management requirements to standardize your corporation's IT architecture and nomenclature. Restart languishing data quality and stewardship initiatives. Upgrade your BI environment by bringing in data mining, predictive analytics and guided decision-making technologies only after you have determined that your basic BI architecture and data designs can support these new capabilities.

Reference:

1. From "Supervisory Guidance on Operational Risk: Advanced Measurement Approaches for Regulatory Capital." July 2003, Office of the Comptroller of the Currency. http://www.occ.treas.gov/ftp/release/2003-53c.pdf.

Claudia Imhoff, Ph.D., is the president and founder of Intelligent Solutions (www.IntelSols.com), a leading consultancy on CRM and business intelligence technologies and strategies. She is a popular speaker and internationally recognized expert and serves as an advisor to many corporations, universities and leading technology companies on these topics. She has co-authored five books and more than 60 articles on these topics. She may be reached at CImhoff@IntelSols.com.