Operational risk event data is the history of incidents that originated from operational risk causes. Leading institutions develop these databases to form the basis for analysis and quantification. The database primarily contains out-of-pocket losses but may also contain “near misses” and pending losses awaiting finalization. The new Basel Accord defines loss databases as a key component of good operational risk management and one of the criteria that an institution must meet to be eligible to use advanced capital models.

Why collect operational loss data? There are three basic reasons to collect a history of loss data.

1. To create or enhance awareness at multiple levels of organization. A basic understanding of exposure and loss experience is a prerequisite for comprehensive and effective operational risk management. A record of losses—accumulating into an aggregated picture of the losses per year by risk and business—provides the baseline for analysis and the value proposition for improvement.

2. The data can be used for empirical analysis. What is happening, what events are repeating, for which products, at what control point, for what causes? This analysis can help direct corrective action to improve the control environment. It also lets experience confirm the qualitative analysis of inherent and actual exposure.

3. The data forms the basis for quantification. The latest thinking in capital models, as verified by the new Basel recommendations, uses loss data and actuarial techniques as the basis to quantify operational risk capital. This is equally applicable for top-down and bottom-up approaches. A three- to five-year loss history will be required for institutions to be eligible to use advanced models for the new Basel Accord.

A Data Collection Strategy

The loss event data we seek is spread throughout the company and affects almost every line item of the P&L statement. A comprehensive data collection program implies significant changes in the way the organization captures and processes loss data. The process described below is illustrated in Figure 1.

What data to collect. To support analysis and quantification, the key data elements to be captured are as follows:

- Date (discovered, booked).
- Description (a few lines describing the event and causes. It should be understandable by others for learning purposes and to meet standards of sharing events with a loss consortium).
- Event and possibly effect categories (for example, the Basel categories or internal categories that can be mapped to them).
- Contributing causes (for example, human error, weak controls, security, training, information technology).
- Total original amount (by effect category).
- Recoveries (for example, operational, legal and insurance, separately identified).
- Business line (internal product/business hierarchy with granularity sufficient to support internal reporting and modeling—for example, to support economic capital and mapping to the standard Basel business lines).
- Control point (where the loss occurred, for example, with customer, pricing, risk approval, trade desk, trade capture, confirmation, operations, settlement, G/L reconciliation).
• How discovered (for example, client, business area, finance, audit, regulator).
• Indicators in effect—both basic scaling indicators and key risk indicators. (This data can then be used to assess correlations between indicators, events, and losses.)

A central loss database. Experience shows that the general ledger (G/L) is not an adequate tool for collecting loss data. Operational risk management requires substantially more detail and reporting and analysis (sorting capabilities) than is supported by ledger systems. Consequently, a separate database typically is constructed to accumulate loss events. This database is fed by a combination of production systems and manual loss data capture and entry processes.

Extracts from production systems. It is easier and more efficient to extract data from production systems to feed the database. Most firms have some data in their systems, but availability will differ from firm to firm. Some common sources are the production loan systems that may record write-offs (for example, to capture credit card fraud), insurance (third-party and captive settlements) and legal case tracking, and settlement systems (for example, to capture penalties). There may be other sources captured in personal computers or specialized databases built by end users. The goal is to build interfaces or extracts from these databases to feed the loss database on a regular basis. Usually, not all the required data elements will be captured. Some can be inferred from the source. Others will have to be recorded after the fact, perhaps with some additional research.

Individual loss capture. There are always events not captured in any production system. They could be one-time events, such as a major reconciliation problem that was recorded with just a journal entry. Other losses, such as those from a trade booking error, may simply appear as part of the P&L volatility unless specifically recorded. Consequently, loss databases should provide for online data entry of events, preferably on a firm’s intranet, to facilitate access across the organization. Such a web-based system might be custom built in house or purchased off the shelf from a vendor. The build-versus-buy decision will usually be driven by the need for customization (both initial and ongoing) versus the need for speed. In either case, running a pilot in a single product or region-based business line increases the likelihood of successful development and implementation across the organization. Such a pilot can be a proof of concept and create evidence for the return on investment. A typical system will allow responsible individuals to describe the event, set the general ledger codes, and get approval from the appropriate manager.

Approval and release. As events are captured or recorded, line managers whose P&L is affected by events should review the entries prior to finalization and their subsequent access by the central risk management function. Losses should be reviewed to ensure that they are applicable to that business area and are coded properly. In addition, they should ensure that descriptions are complete and informative but do not inappropriately identify any individuals or clients. This type of information is not necessary for the typical uses of a loss database and so should be excluded. Approval by business managers releases the event to the central database and also signals that it should be paid (if an external event) and recorded in the general ledger. This process creates a natural control to ensure that losses are recorded. An effective approval-and-release protocol increases the use of the system, assuring managers that they can control the process for approving the loss descriptions, and also improves the quality of the data.

Reconciliation. Some form of reconciliation helps ensure that all data elements have been captured in the loss database. The ideal control is to establish comprehensive general ledger accounts by event category to record all operational losses. The entries in these accounts can then be reconciled against the database to see if anything got into the ledger and bypassed the database or was recorded in the database but not the applicable general ledger account. Changing the general ledger system and accounting procedure to accommodate all operational losses in unique accounts is probably not practical at most large institutions, so an element of memo accounting with manual reconciliation is likely required.

Addressing Cultural Issues
Adoption of a loss reporting strategy implies significant cultural change. The natural inclination is to manage mistakes rather than share and publish them to a broader group. There are some powerful disincentives to participating in a reporting scheme—extra work, skepticism, perhaps a natural desire to forget that the incident ever happened, and above all, lack of trust and the fear of reprisals. Over time, risk managers have
observed some success factors required to overcome these cultural obstacles:¹

- Provide indemnity against disciplinary proceedings to those who caused and reported events. Mistakes are opportunities for improvement, not reasons to shoot the messenger, except in instances of criminal activity or gross policy violations.
- Ensure confidentiality of those involved. Neither the database nor the reporting should reveal the names of any employees involved.
- Separate the department that collects and analyzes the reports from those bodies with the authority to institute disciplinary proceedings and impose sanctions. For example, the Operational Risk department should be separate from Audit if Audit is responsible for incident investigation.
- Provide rapid, useful, accessible, and intelligible feedback to the reporting community. Few things will stifle incident reporting more than the perceived absence of any useful outcome.
- Make data entry as easy as possible.

Other Lessons Learned
In addition to the issues described above, experience has shown that the following points are important success factors in implementing a data collection strategy.

- Build clear definitions of operational risk and related classification criteria. There are gray areas of operational loss between market and credit risk experience, as well as between operational event categories. Some businesses choose to capture events in multiple loss databases. For example, a credit write-off with a loss higher than it would have been, absent operational errors in managing the collateral, would be recorded in both the credit and the operational loss databases. It is essential that the system be designed to allow flagging of these special situations to avoid double counting of losses and a resulting overestimation of economic or, eventually, regulatory capital.
- Capture actual losses only, and segregate the types of recoveries. When modeling capital, do not use estimates in the data history.
- Record all of the losses as one event. Splitting losses among event categories may result in grossly misleading VaR figures.
- Create a system and reporting capability to link multiple related events.
- Determine who is responsible for ensuring complete data capture for each risk category in each business area or staff function. Event research should be distributed in the line and staff organizations. Some institutions require each business to verify that database records are complete.

Summary
Accumulating loss data should be extremely valuable to operational risk management and quantification. The activity is new and implies extensive organizational change. With experience and a disciplined process, we might someday see the same level of accounting standards and transparency over operational risk that exists today for credit risk.

The authors can be reached at Joseph.G.Newberry@citi.com and Mhauby@aol.com.

Notes