



Practical operational risk management: part four — loss data collection

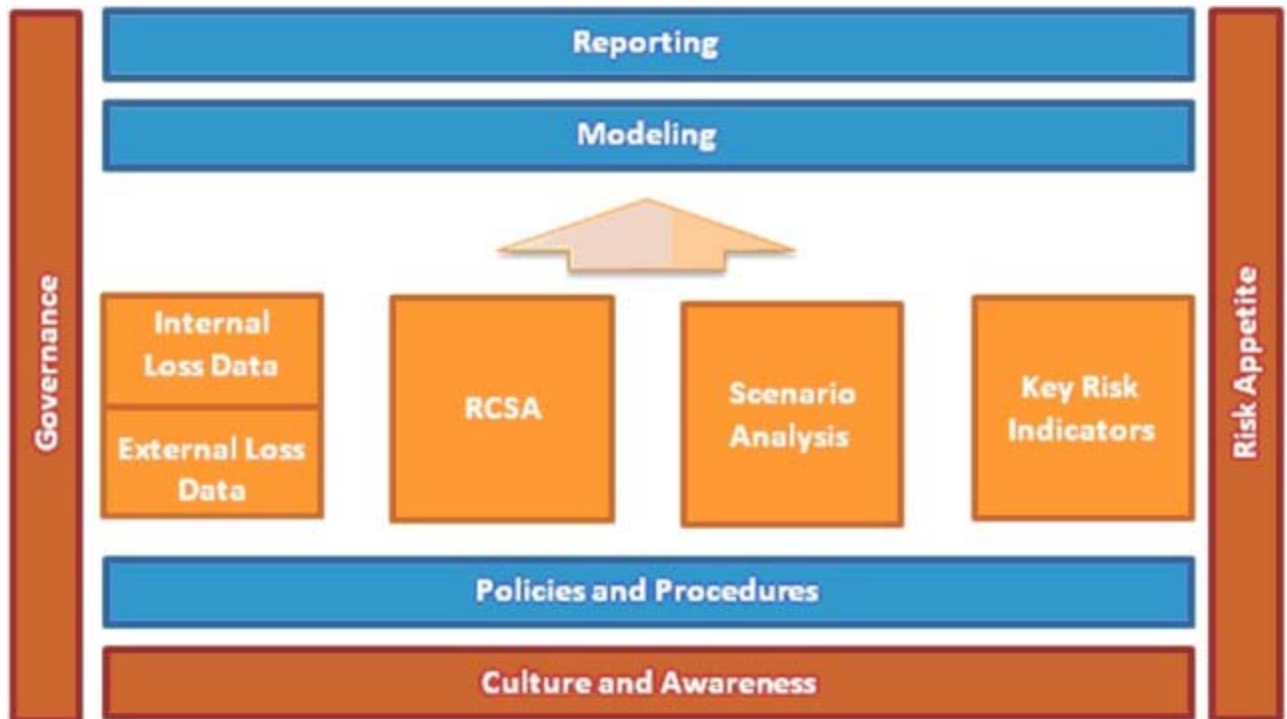
Mar 05 2009 [Philippa Girling](#) *Complinet exclusive*

This article is the fourth in a series on practical operational risk management. The series looks into the practical aspects of building, maintaining and driving forward an effective operational risk management program.



Philippa Girling

The first [article](#) briefly looked at all the elements that are needed for an effective operational risk framework as below:



The [second](#) and [third](#) articles addressed the challenges and opportunities of implementing an effective governance structure and the importance of addressing the cultural change that is necessary to succeed. This article looks at the practical aspects of an effective loss data collection program. Both internal and external loss data play valuable roles in an effective operational risk framework.

Internal loss data

Internal loss data provides insight into what has already happened in a firm. It tells the firm where operational risk has already been experienced and can help it predict where there might be future losses. For this reason, many firms use their internal loss data as the main input into their capital modeling calculations. When a firm designs an appropriate loss data program, it is important that the purpose of the program is understood as this will affect the approach taken. There are several possible purposes and most firms have more than one in mind when implementing a loss data program:

- Collecting data for capital modeling.
- Identifying control weaknesses.
- Understanding current operational risk exposure.
- Embedding the operational risk discipline.

When collecting loss data it is important to consider who, what, where, when and why.

Who?

As operational risk-related losses can occur anywhere in the firm, it is important that the responsibility for reporting such losses is clear and consistent. There needs to be one individual in each department or group who is responsible for ensuring that all loss events are reported in a timely manner. It may also be helpful, however, to adopt an "if you see it, you must report it" policy; or perhaps, more practically, an "if you see it, you must ensure someone reports it" policy.

In other words, once someone is on notice that an event has occurred, they have a responsibility to ensure that it is reported — even if they are not the person to do the reporting. For this type of policy to be successful, the prerequisite training and cultural embedding must have already occurred. The actual reporting of the event will probably belong to an OR coordinator in each area, unless the firm adopts an open access policy under which anyone can report an event.

What?

Any event that meets the definition "loss resulting from failed or inadequate people, process, systems and external events" should be included in a loss database. There may be a threshold over which reporting is mandatory, for example, \$10,000, or a zero threshold might be adopted, which require all events to be recorded. The details that are required for each loss data entry will be driven by the purpose of the loss data program.

A Basel II firm that pursues an advanced measurement approach, however, must adhere to minimum requirements. These requirements are a good standard for any loss data program:

- Every event must be mapped to one of the seven Basel II level one categories.

Event-Type Category (Level 1)	Definition
Internal fraud	Losses due to acts of a type intended to defraud, misappropriate property or circumvent regulations, the law or company policy, excluding diversity/discrimination events, which involves at least one internal party.
External fraud	Losses due to acts of a type intended to defraud, third party
Employment Practices and Workplace Safety	Losses arising from acts inconsistent with employment, health or safety laws or agreements, from payment of personal injury claims or from diversity / discrimination events
Clients, Products & Business Practices	Losses arising from an unintentional or negligent failure to meet a professional obligation to specific clients (including fiduciary and suitability requirements), or from the nature or design of a product.
Damage to Physical Assets	Losses arising from loss or damage to physical assets from natural disaster or other events.
Business Disruption and System Failures	Losses arising from disruption of business or system failures
Execution, Delivery & Process Management	Losses from failed transaction processing or process management, from relations with trade counterparties and vendors

- There must be documented, objective criteria for allocating losses to specified business lines and event types.
- The loss data program must be comprehensive and capture all material activities and exposures from all appropriate sub-systems and geographic locations.
- It must include all material losses that are above a de minimis gross loss threshold, for example, €10,000.
- Each loss data entry must include the following data:

- Loss amount.
 - Date of the event.
 - Any recoveries of gross loss amounts.
 - Descriptive information about the drivers or causes of the loss event.
- There must be specific criteria for assigning loss data that arises from an event in a centralized function (e.g., an information technology department) or an activity that spans more than one business line, as well as from related events over time.
 - Credit risk-related events and market risk-related events should be collected and flagged as boundary events. When using loss data as an input into a capital calculation, credit risk boundary events can be excluded from the calculation, but market risk events must be included.

Additional reporting requirements can be added, such as:

- Action items, with owners and due dates to mitigate the impact of this event and/or to prevent its recurrence.
- Non-financial impacts, such as reputational impact.
- The identification of all involved departments.
- Details on additional indirect costs, such as legal fees.

When a firm determines what should be included in loss reporting, it may conclude that as well as financial losses, it would benefit from collecting information on gains, near-misses or losses that have a non-financial impact only. Many firms have taken this broader approach to loss data collection and have, therefore, named this program operational risk event capture rather than loss data capture.

Some firms also include balance sheet or profit and loss adjustments as loss events. There is some discussion as to whether these are actual losses, "timing events" or "accounting adjustments". It is up to the firm to determine whether the collection of such events meets the purpose of its operational risk event program.

Where?

Most firms started their operational risk event capture programs in spreadsheets, and then quickly determined that a more sophisticated and robust system was needed. As a result, there are many operational risk event or loss database software vendors today which offer flexible and proven systems. Many firms have determined, however, that they need to build in-house systems to meet their unique requirements. Whether a vendor-provided or an in-house built system is selected, it is inevitable that a firm will need a technology solution to effectively capture and manage operational risk events.

When?

Operational risk event reporting relies on timely participation across the firm. It is generally appropriate to have a policy that requires immediate reporting of an event. It may be necessary, however, to set up complex workflow to allow departments to review and approve their operational risk events before signing off on them and passing them to a central operational risk function for analysis and tracking.

Why?

The purpose of an operational risk event collection program must be clear, and must be part of culture and

awareness activities.

External loss data

Events that occur outside a firm can provide insight into risks that a firm faces, and can provide valuable input. As with internal events, when designing an appropriate external loss data program for a firm, it is important to understand the purpose of the program as this will affect the approach taken. Once again, there are several possible purposes and most firms have more than one in mind when implementing an external loss data program:

- Collecting data for capital modeling.
- Identifying control weaknesses.
- Understanding current operational risk exposure.
- Embedding the operational risk discipline.

External losses can be used as a direct input into a capital model for a Basel II firm, but more often external loss data is used to inform other parts of the operational risk program. For example, operational risk events that have occurred in a certain industry may provide examples for a firm's scenario analysis and risk and control self-assessment programs. External events are often of great interest to senior managers. Bad things that have happened to other people can generate healthy discussion about the operational risk exposures that exist in a firm, and so these should be included in regular reporting.

There are several sources of external operational risk event data. Relevant alerts on internet search engines and online newspapers and journals can be set up so that a firm receives an e-mail whenever an event occurs that includes a keyword or company name that has been specified. A firm can also subscribe to online and printed journals and newspapers, and receive regular e-mails from them that summarize current events. In addition, there are several providers of operational risk event information, which include SAS and Algorithmics Fitch First, that offer fee-based operational risk event data services. There are also consortium-based operational risk event services, such as ORX which provides benchmarking operational risk event data to its member banks.

There are several challenges with external data. First, there is a bias in reporting that results in the reporting of events in the press which are press-worthy, such as large scale fraud, with less coverage on less salacious events, such as systems outages. Secondly, it can be difficult to determine whether an event is relevant to a firm. Rather than checking to see if the exact same event could occur within the firm, therefore, it is more important to carefully analyse external events to determine if there are any lessons to be learned. Internal and external operational risk events provide an excellent window into what has already gone wrong. We can learn from them, put in place mitigating actions to prevent them and make changes to protect firms from future similar events. They can also provide excellent data for the calculation of operational risk capital.

- **Philippa Girling** is an Of Counsel Attorney at Garrity, Graham, Murphy, Garofalo and Flinn in New York. She was previously global co-head of operational risk management at Nomura.

This article first appeared on Complanet on www.complanet.com on March 05 2009. For a free trial of Complanet's services, please contact client support on client.support@complanet.com or +44 (0) 870 042 6400.