
SOCIETY OF ACTUARIES

Article from:

# Risk Management

August 2008 – Issue No. 13

# Risk Identification: A Critical First Step in Enterprise Risk Management

*Sim Segal*

Enterprise Risk Management (ERM) is often defined as a process to identify, measure, manage and disclose all key risks to increase value to stakeholders. ERM is still an emerging concept, and those companies adopting it are in varying stages of implementation. The first phase in the ERM process cycle, after developing the initial ERM framework and plan, is risk identification.

Risk identification typically involves three types of activities:

- Defining and categorizing risks;
- Conducting internal qualitative surveys on the frequency and severity of each risk; and
- Scanning the external environment for emerging risks.

Since risk identification is the first phase in the ERM cycle, some assume that by now the approach must have matured, and that common practice is essentially "best practice." However, through our research and client work, we have found that common practice in risk identification is suboptimal in several aspects, and produces misleading information not only in risk identification, but also in all downstream ERM phases: risk quantification, risk management and risk disclosure. Relying upon this flawed information puts management at risk of:

- Focusing on the wrong priorities;
- Making poor decisions; and
- Producing improper risk disclosures.

To have a successful ERM risk identification phase and avoid these problems, companies must:

1. Define risks by source
2. Categorize risks with consistent granularity
3. Identify risks prospectively
4. Gather data appropriately
5. Define frequency-severity clearly

## Defining Risks by Source

Risks are often defined by their outcome rather than their source. For example, "reputation risk" is a risk commonly found on a company's key risk list. However, this is not a source of risk, but rather an outcome of other risks. There are several risks—such as poor product quality, poor service, fraud, etc.—that might rise to a level whereby reputation is negatively impacted.

Another example is "ratings downgrade." Again, this is not a source of risk, but an outcome that can result from several different risk sources, e.g., strategy risk, execution risk, etc. A poor strategy, for example, might result in a rating agency downgrading the company.

This is a common practice, yet defining risks by their outcome, rather than their source, results in several suboptimal ERM steps. It degrades the qualitative survey results; survey participants have an inconsistent understanding of the risk they are assessing, since each person may be considering a different risk source and scenario triggering the event. This also makes risk quantification more challenging and uneven; risk experts have difficulty constructing specific risk scenarios for quantification, since the risk is defined so ambiguously. Finally, management struggles to identify and evaluate mitigation alternatives, since risks are generally mitigated at the source rather than the outcome. For example, it's easier to consider mitigation of potential sources of reputation risk (e.g., poor product quality, poor service, internal fraud) than it is to mitigate an amorphous concept like reputation damage in the abstract.

**continued on page 30**

Sim Segal, FSA, CERA, MAAA, is US Leader of ERM Services at Watson Wyatt in New York. He can be reached at *sim.segal@watsonwyatt.com.*

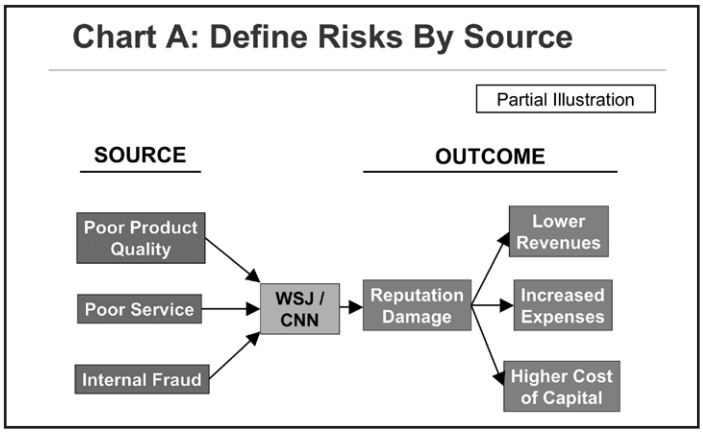
# Risk ID: A Critical First Step

## Risk Identification ...

◗ continued from page 29

To avoid these difficulties, management must define risks by their source. In our prior example of "reputation risk," we listed three examples of risk sources that might involve reputation damage in an extreme scenario. Chart A shows these risks along with a partial illustration of the relationship of risk sources to intermediate impact(s) and to outcomes. In the chart, the arrows show how each risk can trigger media coverage, resulting in reputation damage, followed by financial repercussions.

**Chart A: Define Risks By Source**




With risks defined by their source, the ERM steps flow well. There is data integrity in the qualitative survey; since each risk is clearly defined by its source, survey participants have a consistent understanding of each risk, resulting in a coherent assessment. This also makes risk quantification easier. Since risks are defined so clearly—each with its own specific source—risk experts can more easily develop risk scenarios, following logical downstream impacts from each originating source. Finally, management can clearly identify and evaluate both pre-event and post-event mitigation alternatives, since both the source of risk and the downstream events are apparent.

**Chart B: Consistent Granularity**

| CATEGORY: OPERATIONAL RISK<br>Sub-Category: Human Resources Risk | Partial Illustration |
|---|---|
| Employee productivity | Employees not performing at the level of productivity expected |
| - Training & development | Training and development program not matching expectations |
| - Change management | Management unable to lead cultural changes as planned |
| - Organizational structure | Org structure results in productivity not matching expectations |
| Talent management | Management of talent not matching expectations |
| - Ability to recruit / retain | Ability to recruit or retain staff not matching expectations |
| - Succession planning | Ability to develop new leadership not matching expectations |
| - Critical employees | Unexpected loss of critical-path employees (unique knowledge/skills) |
| - Labor/producer relations | Employees/unions or producers take unexpected action against firm |
| Conduct | Poor or criminal conduct by employee/management |
| - Public behavior | Poor public behavior by employees or management |
| - Internal fraud | Fraud/theft by employee or management (other than I/T-related) |
| - Internal destructive acts | Destruction of company property (not I/T-related) by employee / mgmt |

## Categorizing Risks with Consistent Granularity

Risks are often categorized with inconsistent levels of granularity—either at too high a level or too low a level.

It is common to find a risk list that includes some risks defined at too high a level of abstraction—the risk is really a category of risks that should be refined into a set of smaller, individual component risks. For example, "talent management" —a type of human resources risk—should be broken down into its individual risks, such as "ability to recruit/retain," "succession planning," etc.

Defining risks at too high a level, results in suboptimal internal qualitative surveys. It leads to uneven scoring by survey participants, since the larger category obscures its several component risks. However, when risks are consistently defined at the individual risk level, the assessment is more meaningful, since participants can consider and assess each risk individually.

It is even more common to find risks defined at too low a level of abstraction—the risk is really only one of a larger category of risks. For example, "lack of innovative products" is only one specific risk in a larger category. This should be elevated to a higher level of abstraction, and included in the category of "strategy execution."

Defining risks at too low a level, threatens the environmental scanning activity. It can cause a failure to identify all related types of risk in the larger category. In our example, management may not have considered other risks to strategy execution, for example, "inability to achieve planned growth," "failure to expand into key new markets," etc.

A partial example of how to categorize risks at a consistent level of granularity is shown in Chart B for human resources risks.

## Identifying Risks Prospectively

Risks are often identified retrospectively. Some risks are on the key risk list merely because they occurred recently and management wants to see them there. This is called "fighting the last battle" syndrome. In addition, these risks are often defined at too low a level of granularity, since they are descriptive of the recent specific event.

Including these on the risk list, in this way, can skew the qualitative survey results. These risks are often over-weighted; participants are more sensitized to them and are not fully aware of the mitigation that has likely been put in place following the recent occurrence. Retrospectively defining risks also negatively impacts environmental scanning; it is a distraction from identifying the next risk event (as opposed to the last risk event).

Identifying risks prospectively can help avoid these difficulties. It reduces some of the bias in the risk assessment, by not confusing recent experience with future likelihood and impact. It also focuses management away from the past, and concentrates attention on what might impact the company's ability to deliver on its strategic objectives going forward. This enables a robust, untainted examination of where the company is, where it's headed and what could get in the way.

## Gathering Data Appropriately

In the risk identification phase, qualitative survey participants are usually asked to assess the frequency and severity of a large list of risks. However, in most cases, there is also an attempt to gather a large amount of additional data at this stage: key risk indicators; exposure metrics; historical frequency and severity; current mitigation in place; planned mitigation; anecdotal experience at competitors, etc.

However, it is counter-productive to gather all this data during the risk identification phase. Too much data is gathered. Most of this data is only needed for the key risks, rather than the long list of risks provided to survey participants. The primary purpose of the risk identification phase is to prioritize—to narrow down a list of (potentially hundreds of) risks to those key risks that will go to the next ERM phases: risk quantification, risk management and risk disclosure. All that is needed for prioritization is the frequency-severity scoring.

In addition, the data is collected too early. The data that is needed—the data for the key risks—is not needed until the risk quantification phase because it is used to develop and quantify risk scenarios. Since the data is collected too early, it is often deposited in a database where it languishes and as time passes, the quality decreases.

Finally, the burden of the shear volume of data requested results in survey fatigue. this overwhelms survey participants and decreases the quality of the critical input—frequency and severity assessment.

These difficulties can be resolved by gathering the appropriate data at the proper stage in the ERM process. In the risk identification phase, the qualitative survey should focus participants primarily on assessing frequency and severity. At the risk quantification phase, data should be gathered for developing and quantifying risk scenarios for the key risks. This avoids gathering too much data, since the larger data request is not unnecessarily performed for those risks that are not key risks. In addition, data is more current, since it is gathered closer to the time it is needed. Finally, survey participants can do a better job, since they are not overwhelmed by excessive volume.

**continued on page 32**

Risk Identification ...

◗ continued from page 31

**Chart C: Illustrative Scoring Criteria**

| Frequency | Severity |
|---|---|
| 5 = Very High | 5 = Impact of $100M+ |
| 4 = High | 4 = Impact of $50M - $100M |
| 3 =Moderate | 3 = Impact of $25M - $50M |
| 2 = Low | 4 = Impact of $10M - $25M |
| 1 = Very low | 5 = Impact of less than $10M |

## Defining Frequency-Severity Clearly

When survey participants are asked to qualitatively assess a list of potential risks, the most common approach is to ask them to score each risk on both a frequency and severity scale. Guidance is usually provided in terms of scoring criteria. A simplified example is shown in Chart C.

However, this approach often results in disparate impressions among survey participants as to how to score both frequency and severity, negatively impacting survey results.

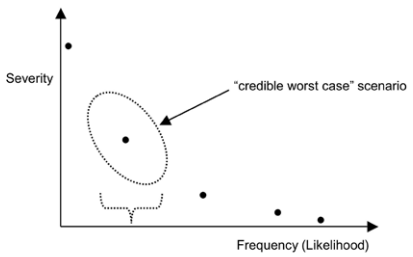
To score frequency, participants must consider a specific risk scenario. Is it an end-of-the world scenario? Is it a most likely scenario? The former would solicit a lower frequency score than the latter. However, such guidance is rarely provided. As a result, each participant tends to imagine a different scenario, and collectively they are essentially not scoring frequency for the same risk event.

To score severity, participants must understand the metric impacted. Is it an earnings hit? Is it one-time or cumulative hit (and for how many years)? Is it a capital hit? Is it a hit to market capitalization? While guidance usually includes magnitude, as in our example, sufficient detail regarding the impact is often omitted. Again, participants have an inconsistent understanding and are not assessing on the same basis.

To resolve this, it is important to more clearly define frequency and severity prior to the qualitative risk assessment.

To define frequency clearly, participants must be given guidance as to the type of risk scenario to consider. One example of how to do this is to focus participants on a particular type of risk event, as shown in Chart D. A range of data points is shown in the chart, each representing a potential risk event. The ellipse illustrates that survey participants should consider a "credible worst case"—not an (extremely unlikely) end-of-the-world event and not an event that occurs with moderate frequency.

**Chart D: Guidance on Frequency**




To more clearly define severity, more specificity should be provided on the metric(s) intended. A leading practice is to express the scoring criteria in terms of a single metric that can capture all potential impacts—impacts to income statement, balance sheet, required capital and cost of capital. The only metric that captures all of these impacts appropriately is enterprise value—the present value of projected cash and capital flows into the future, where the projection is consistent with the strategic plan. This is not market capitalization. Rather, it is the value an investor should pay today, if the company were to perfectly execute its strategic plan and everything go precisely as expected.

The enterprise value metric is initially less tangible to some, since it's a complex calculation. However, it is intuitive—the value of the firm is a concept everyone understands. In addition, simple illustrations of selected risk events and their relative impact on enterprise value provide survey participants with a general feel for this metric that is sufficient for qualitative assessment purposes.

Though risk identification is the first step in the ERM process cycle, appears to be the simplest, and is the most traveled, common practices are fraught with issues that can damage an ERM program. To avoid this, management must: define risks by source; categorize risks with consistent granularity; identify risks prospectively; gather data appropriately; and define frequency-severity clearly. Companies adopting these "better practices" have found that the risk identification phase is quicker, easier, more widely understood and produces higher quality results, paying dividends as well in downstream ERM phases. Those continuing with common practices may find themselves more at risk—of focusing on the wrong priorities, making poor mitigation decisions, and ultimately improper risk disclosures. ✦