Organizational Risk Profile Measurement & Management

Andrew D. Banasiewicz, Ph.D.
Boston University

Introduction

All business, as well as other organizations, face multitudes of risks. Some of those risks, most notably credit or currency exposures received a considerable amount of attention, which ultimately led to the emergence and the proliferation of objective assessment tools; even the inherently difficult to forecast natural disasters, such as violent storms or earthquakes, are being quantitatively modeled. However, surprisingly little analytical effort has been directed toward other exposures, such as operational and strategic risks, in spite of the potentially profound impact those threats can have on organizational well-being. In a very practical sense, this informational deficiency hampers organizations' abilities to establish holistic risk management practices, especially as it relates to measurement and tracking-intensive enterprise risk management (ERM).

One of the difficulties associated with systematically assessing organizations' exposure to operational and strategic risks is those risks' heterogeneous plurality, the consequence of which is that the sheer number of distinct threats can be overwhelming. A potential solution to that problem is to think of organizations as "bundles of risks", where each organization can be described in terms of its own unique *risk profile*. Defined as a composite of the potentialities of bad (i.e., downside) and good (i.e., upside) risks, organization-specific risk profile will highlight the most pronounced, in terms of the likelihood of occurrence and/or the severity of impact, threats facing an organization, in addition to offering means of cross-organization differentiation. Hence in a comparative sense, if the organization's total risk exposure is greater than that of its competitors, or if its total cost of risk is higher than that of its competitors, that organization's earnings—and ultimately, its competitiveness—can be adverse effected.

Risk Profile Measurement

Considered from an analytical point of view, risk profiling demands *entity-specific estimation*, which focuses data analytic efforts on the derivation of organization-specific, rather than aggregate (as in actuarial analyses) effects. That requirement might seem self-evident, but many aspects of risk management continue to rely on aggregate generalizations, such as those used in economic or actuarial analyses. For instance, when assessing exposure to shareholder litigation (a major executive risk in the U.S, now slowly beginning to emerge in some of the EU countries), it is common to make use of company grouping attributes such as industry membership (e.g., Global Industry Classification Standard) or size (i.e., its market capitalization or revenue) for the purposes of exposure estimation. Companies with shared communalities on those or other generic attributes form risk clusters which may include as few as several dozen or as many as several hundred of individual organizations – all companies that fall into a cluster are then deemed to exhibit essentially the same exposure to a particular risk. The old adage – correlation is not causation – captures the fallacy of such analytically-coarse approach: Just because more companies of a particular size or in a particular industry incurred more of certain events does not mean that the underlying causes were size or industry membership.

In order to differentiate between mere correlates and more informationally meaningful causal factors, risk profiling should utilize (in situations where the requisite data are available) *explanation-based prediction*, rather than trend extrapolation. This process is inherently reductive, which is to say it decomposes individual risks into their constituent, lower level components, all with the goal of identifying specific indicators that can be used to estimate the likelihood and the severity of events of interest.

Key Estimation Considerations

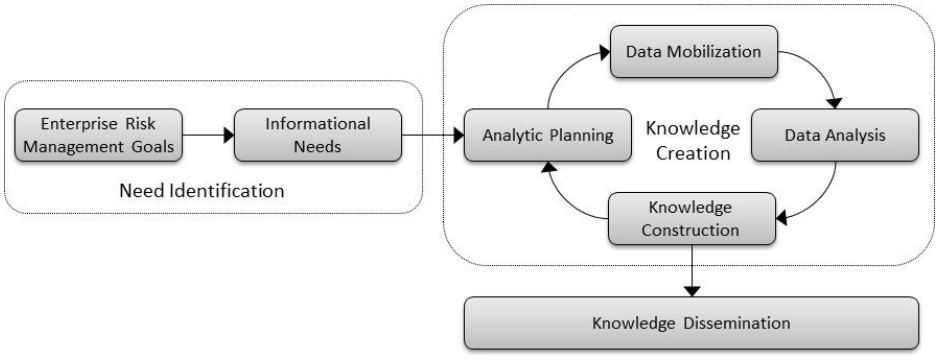
The two framing aspects of the risk analytics approach described in this book—explanation-based prediction and entity-specific estimation—carry a number of implications. First, the estimation of the likelihood and severity of outcomes of interest entails the use of multiple metrics, both quantitative and qualitative, the goal of which is to enhance the accuracy of future states' predictions and the completeness of the underlying causal explanation. Second, analytic conclusions should be geared toward improving the efficacy of future decisions, as measured in terms of the expected impact on earnings. Third, the interrelationships among the individually estimated risk types should be assessed in the context of a dynamic system capable of propagating future changes.

Method-wise, the above implications of the two key framing aspects of risk profiling translate into the following recommendations:

1. *Focus on multi-source, multivariate analyses.* Risk types vary widely in terms of their nature, the overall frequency of occurrence and the availability of ready-to-use data. Multi-source data are a necessary prerequisite to simultaneous assessment of the totality of the organization's risk exposure; multivariate analyses, on the other hand, are necessary to the development of reliable explanation-sourced forward-looking prediction of likelihood and severity of individual risk types.
2. *Qualitative estimation of risk types for which no reliable quantitative data exists.* Numerous threats (e.g., pandemics, terrorism) are characterized by sparse, analytically prohibitively limited data, which impedes the use of multivariate analyses discussed above. In those situations, rather than relying on non-generalizable or otherwise inadequate data, likelihood and impact estimation should leverage " qualitatively constructed" data, generated using proven subjectivity-dampening techniques, such as the Delphi method.
3. *Estimation of cross-risk interrelationships, supporting system-wide propagation of future changes.* One of the key premises of risk profiling is that individually estimated risk types are subsequently integrated into a composite system, which makes possible the estimation of cross-risk type interdependencies. Furthermore, in order to accommodate ongoing updates, the risk assessment system should also be capable of propagating changes to one or more "connections" onto the entire network, as is the case in Bayesian belief networks.

The Overall Risk Profile Measurement Process

A high level view of the risk profile measurement process is graphically depicted below. The overall risk analytical process is comprised of seven distinct components, which are grouped into three explicit categories: 1. *Need Identification*, 2. *Knowledge Creation*, and 3. *Knowledge Dissemination.* The goal of the Need Identification part of the overall risk analytical process is twofold: First, it is to bring forth the agreed upon risk management goals and priorities of the organization. To be clear, the focus of this step is simply on delineating – as opposed to deriving – the individual objectives that have been embraced by the organization. Second, it is to translate the delineated strategic objectives into specific informational goals. Implicitly, this step recognizes that a successful achievement of the organizational goals is, to a large



degree, dependent on the attainment of a high degree of decision making clarity. Hence, the overall objective of the Need Identification stage of the risk analytical process is to distill the agreed upon risk management goals into a clear set of informational demands.

The goal of the second, broad stage of the risk analytical process—Knowledge Creation—is that of fulfilling the informational demands identified earlier. That is both a tall order and a very broadly scoped endeavor. As graphically shown above, it encompasses four distinct process-linked components: Analytic Planning, Data Mobilization, Data Analysis and Knowledge Construction. It is an iterative process which continues to refresh data-derived knowledge supporting current goals, or generates new knowledge for updated or newly established goals. In a sense, this is the "engine" of the risk measurement process, and it is the source of risk profiles discussed earlier.

Lastly, the risk analytical process culminates in the Knowledge Dissemination step, a deceptively simple, logical conclusion to the overall progression. To say that it is deceptively simple is akin to saying that its importance is frequently overlooked, which can lead to informationally-rich insights having unjustifiably little decision-guiding impact.

Risk Profile Management

Ultimately, any risk response decision should be considered in the context of risk-return tradeoff. At least in theory it is possible for an organization to enter into a large number of financial contracts which would either outright transfer the risk or provide post-event compensatory mechanisms, so much so that the said organization would be shielded against a vast majority of loss causing events. However, the overall cost would be more than likely prohibitively high, so that from the economic standpoint that would not be a plausible scenario. Hence basic economics, in effect, force organizations into deciding which risks to transfer, which ones should be considered avoidable, or at least mitigatable, and which ones simply need to be accepted. Combining thoughtful risk delineation and reliable organization-specific impact estimation with sound financial decisioning is thus at the heart of risk profile management.

Risk Acceptance

The willingness to participate in a competitive marketplace implies willingness to accept a certain amount of risk. More specifically, it entails the acceptance of the upside component of the overall risk, which are threats that emanate from organizations' strategic decisions. For instance, an auto manufacturer developing (i.e., investing in) an alternative fuel-powered automobile implicitly assumes the (strategic) risk associated with the future viability of that particular approach. In other words, the organization makes a strategic decision and then it implicitly assumes the risk of that decision leading to a loss rather than profit; implicitly, the organization also assumes the opportunity risk, which is the risk of choosing to pursue, let's say, bio fuel- rather than electricity-powered engine development.

From the point of view of risk management, the core consideration that underpins the decision to accept a particular risk is that it is a reasoned outcome of informed decisioning – stated differently, it should not be a product of inaction (ultimately leading to a de facto acceptance). Every delineated risk's response ought to follow the risk's inherent characteristics, thus the decision to accept should be supported by objective evidence.

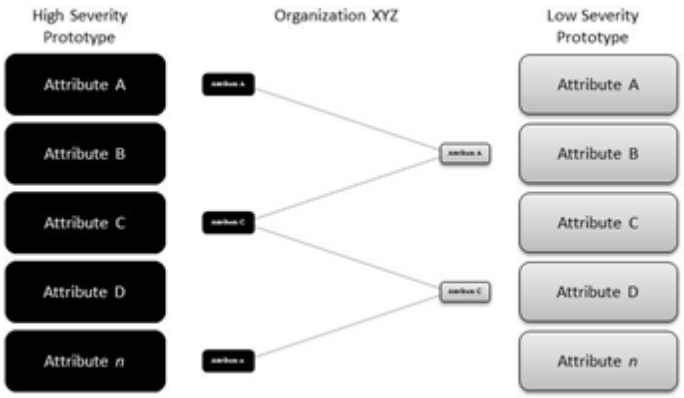
Risk Transfer

Commercial insurance is perhaps the most widely used form of risk transfer, and to many risk managers it is the most intuitively obvious risk response mechanism, though it is also tends to be the most costly. (It could be argued that since the purchase of insurance coverage does not change the likelihood of an adverse event materializing it might be more appropriate to think of insurance as a post-event compensatory mechanism; however, the ensuing analysis will adhere to the conventional view of insurance as a risk transfer tool.)

In general, risk transfer entails the use of a wide range of financial tools – in addition to commercial insurance, organizations can select from an array of alternative mechanisms, such as captive insurance, hedge funds, contingent capital, securitization, to name just a few. The choice of any of the available risk transfer options rests on the key consideration: What is the tradeoff between the speculative chance of incurring a cost-bearing event and the non-speculative (i.e., definitive) cost of purchasing a risk transfer contract? In practice, the prevailing market conditions, in conjunction with the organization's creditworthiness will effectively set the purchaser- and risk-specific transfer price; however, the probabilistic likelihood of occurrence and severity of impact estimates are inherently imprecise. As a result, the aforementioned tradeoff needs to be expressed as a range, or more specifically, a confidence interval (for estimates based solely on data) or a credible interval (for estimates stemming from Bayesian inference).

Risk Avoidance & Reduction

As noted earlier, risk profile is a mix of risk exposure-effecting organizational traits. To the degree to which risk profiling is based on similarity (to prototypical high and low risk exposure entities) analysis, some of the organizational profile-defining attributes will be indicative of high risk, while others will be indicative low risk, as shown in the graphic to the right. Hence it follows that some of the organization's characteristics can be thought of as increasing its risk exposure, while some others as lowering it. Furthermore, both the risk heightening and risk lowering attributes will typically vary in terms of their strength of their impact, which suggests the need for differentiated treatment of the individual risk exposure-indicating organizational attributes. Altogether, taking advantage of the more granular information contained in the organization-specific risk profile will enable the delineation of specific organizational attributes that can be "tweaked" to decrease, or even altogether eliminate the chances of incurring specific adverse events.



In contrast to risk transfer, which nearly always entails additional expenditures, risk profiling supported risk avoidance and reduction are focused on extracting additional value out of already available informational assets. As implied by the two foundations of risk profile measurement discussed earlier – entity-specific estimation and explanation-based prediction – risk profiling delivers far greater informational depth and precision than the widely-used aggregate outcome based analyses, which in turn supports more specific decision-guiding insights.