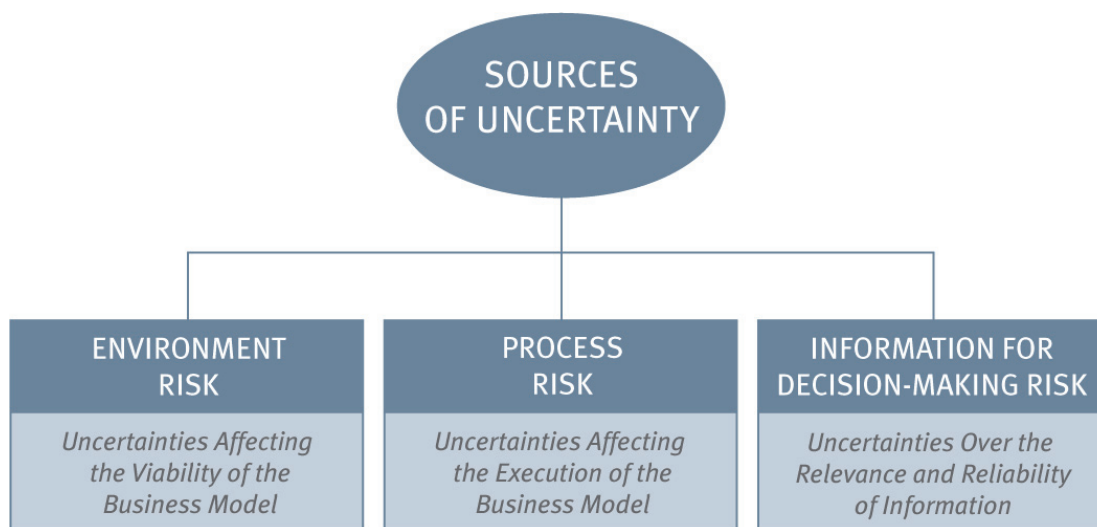


## **The Protiviti Risk Model<sup>SM</sup> – An Illustrative Risk Language**

The topic covered by Issue 2 of Volume 3 of *The Bulletin* is “Credit Rating Analysis of Enterprise Risk Management at Nonfinancial Companies: Are You Ready?” Explored is how consideration of ERM quality can impact the credit ratings process, and what nonfinancial companies can do to prepare for this added dimension. Issue 2 refers to an example risk model to illustrate the potential risks to consider when implementing ERM. Following is an explanation of this model.

Risk is about knowledge, and when management lacks knowledge, there is greater uncertainty. The sources of uncertainty an enterprise must understand and manage may be external or internal, and may relate to the relevance and reliability of information about the external and internal environments. Three broad risk groups – environment, process, and information for decision-making – provide the basis for a risk model summarizing the sources of uncertainty in a business.



Environment risk arises when external forces can affect the entity's performance, or make obsolete or ineffective the entity's choices regarding its strategies, operations, customer and supplier relationships, organizational structure or financing. These external forces include the actions of competitors and regulators, shifts in market prices, technological innovation, changes in industry fundamentals, the availability of capital and other factors outside the company's direct control. They also include catastrophic loss, which will be discussed in detail later.

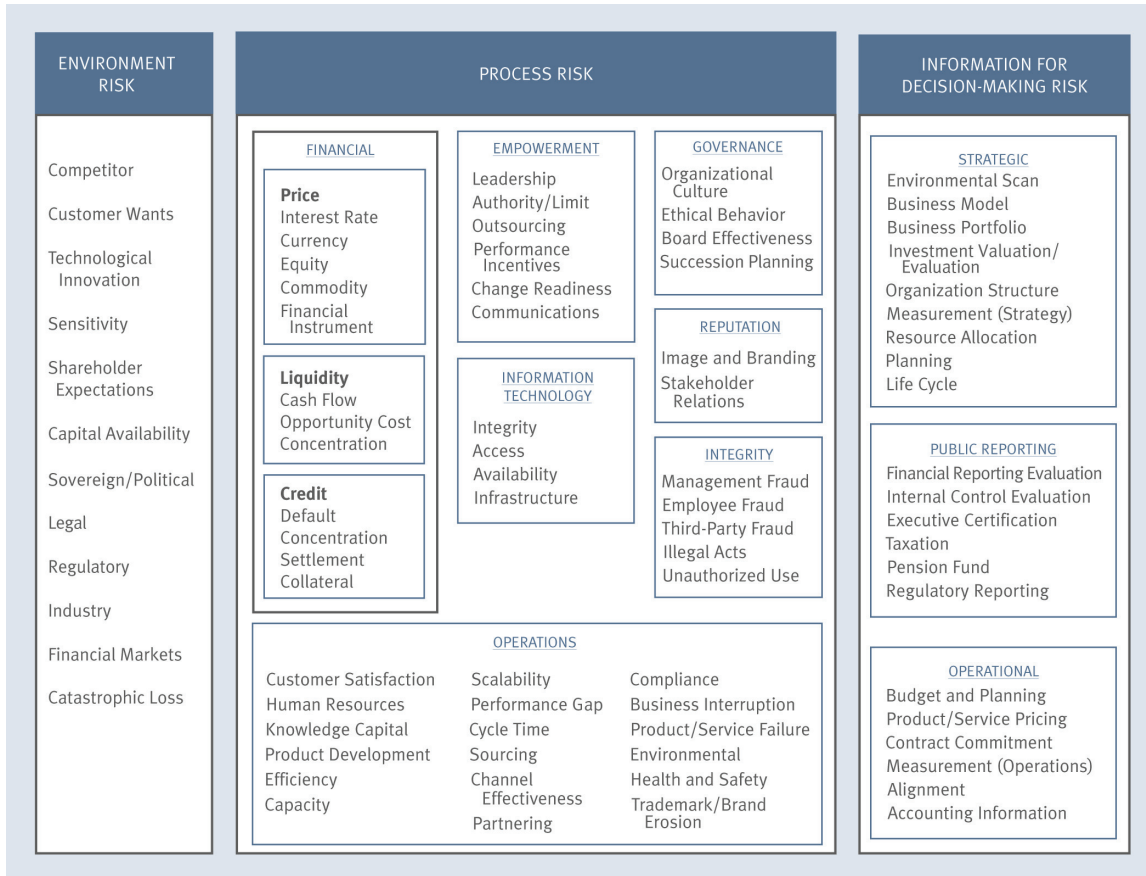
Process risk arises when internal processes do not achieve the objectives they were designed to meet in supporting the entity's business model. Characteristics of underperforming processes, or process risks, include poor alignment with business objectives and strategies, dissatisfied customers and inefficient operations. They also include diluting (instead of creating or preserving) enterprise value and failing to protect significant financial, physical, customer, employee/supplier, knowledge and information assets from unacceptable losses, risk-taking, misappropriation or misuse.

Information for decision-making risk arises when information used to support business decisions is incomplete, out of date, inaccurate, late or simply irrelevant to the decision-making process. Since decisions are made to create and protect enterprise value, these risks are uncertainties that can lead to bad decisions. Poor decisions can lead to risk-taking that is out of line with realistically expected rewards.

These three groupings of risk are interrelated. The environment risks and process risks the enterprise faces are driven by the external and internal realities of the business. Information for decision-making risk is affected directly by the effectiveness and reliability of information processing systems and informal "intelligence gathering" processes for capturing relevant data, converting it to information and providing that information to the appropriate managers on a timely basis. Process risk is sometimes indistinguishable from information for decision-making risk because information is needed to make informed decisions about the performance of a process.

In summary, these three groupings of risk provide a broad foundation on which more specific categories of risk can be identified and detailed. The three groupings of risk are depicted using the risk model shown below.

### Protiviti Risk Model<sup>SM</sup>



Using this model, examples of events may be identified within each relevant risk category listed. For example, catastrophic loss risk is the inability to sustain operations, provide essential products and services, or recover operating costs as a result of a major disaster. The inability to recover from such an event in a world-class manner could damage a company’s reputation, its ability to obtain capital and its investor relationships. There are two sources of events that can lead to catastrophic loss:

- **Uncontrollable events:** Disasters from war, terrorism, fire, earthquake, severe weather, flooding, a pandemic and other similar events that are completely beyond the control of management. Although these events are uncontrollable, management’s

task is to minimize their effect(s) on the organization's assets and operations should they occur.

- Controllable events: Some events can be as catastrophic in their effects on a business as an uncontrollable disaster. These events include environmental disasters; pervasive health and safety violations; spectacularly large underwater real estate deals; headline-grabbing, high litigation costs; huge losses from derivatives; unbridled credit granting; massive business fraud; and significant losses in market share due to failure to abandon strategies that no longer work. The business activities that contribute to these events are within the control of the company. Unmitigated, these events can lead to reputation loss.

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) recommends a “top down” approach to identifying risks in its Enterprise Risk Management – Integrated Framework. This means that management defines the objectives of the organization and the related risk categories impacting those objectives. Specific events are then identified within each category. Thus, the use of a common risk language begins at a strategic level, starting with a model like the one above, and then customizing it to the unique circumstances of each business unit. A well-conceptualized model is a springboard to deeper discussion and understanding of risk. It provides an essential step or “building block” toward an effective ERM infrastructure.

Our experience has shown that a risk language should be adapted to each industry. In fact, we have adapted the Protiviti Risk Model<sup>SM</sup> to more than 30 industries. We also have noted that management can adapt the model for a given industry to their specific company's circumstances. In the adaptation process, the external environment risks and the operations risk tend to take on the specific taxonomy of the industry. Financial risks tend to be selected according to the nature of the industry. The remaining risk categories are relatively consistent across most industries; the question is which risk categories does management want to stress on an enterprise basis.

The point in the above discussion is that companies need a common risk language with which to begin an enterprise risk assessment. They should start with the key risks

provided by Standard & Poor's (S&P), as discussed in Issue 2, Volume 3 of *The Bulletin* and more fully explained in the S&P *Request for Comment: Enterprise Risk Management Analysis for Credit Ratings of Nonfinancial Companies*. They should add additional risks germane to the successful execution of the organization's business model. Examples of such risks are found in the Protiviti Risk Model<sup>SM</sup>. The resulting risk model would provide an excellent context for the application of S&P's PIM (policies, infrastructure and methodology) approach.

© 2008 Protiviti Inc. An Equal Opportunity Employer

*Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services.*