

Credit Rating Analysis of Enterprise Risk Management at Nonfinancial Companies: Are You Ready?

Note: This issue of The Bulletin has been updated in response to Standard & Poor's May 7, 2008, release that articulates the agency's plans to apply enterprise risk analysis to its corporate ratings. This publication supersedes the original Issue 2.

Enterprise risk management (ERM) initiatives have gained strong support from a new source: credit rating analysts. In November 2007, Standard & Poor's (S&P) issued its *Request for Comment: Enterprise Risk Management Analysis for Credit Ratings of Nonfinancial Companies* (RFC), reflecting the rating service's intention to assign scores of ERM quality to all companies it reviews and incorporate an ERM segment into its ratings reports. In May 2008, after receiving comments from more than 60 respondents, S&P released *Enterprise Risk Management: Standard & Poor's to Apply Enterprise Risk Analysis to Corporate Ratings*, in which the original proposal was revised.

Considering ERM in the ratings process is not new. Like Moody's Investors Service, S&P always has probed the risk management processes of financial institutions and insurers. In recent years, both S&P and Moody's have extended their formal evaluation of these processes to entities using an ERM-like framework. Moody's reports that it integrates risk management capabilities into all its credit ratings. Meanwhile, S&P has begun extending the consideration of ERM to power generation companies. Finally, other rating services disclose that they consider various aspects of ERM in their ratings of insurers and financial institutions.

S&P's decision to enhance its ratings process on a global basis for nonfinancial companies could, over time, affect thousands of public and private companies in dozens of industries by expanding the evaluation of ERM capabilities into nonfinancial sectors. The plan released in May 2008 differs from the November 2007 proposal in that it is a more incremental approach to incorporating a comprehensive ERM assessment into the ratings process. However, S&P's overall intent does not appear to have changed substantially. The change in timeline affords nonfinancial companies valuable time to mature their ERM processes. This issue of *The Bulletin*

explores how consideration of ERM quality can impact the ratings process and what nonfinancial companies can do to prepare for this added dimension to the process.

S&P's point of view

In the aftermath of Hurricane Katrina, the recent massive product recalls by reputable companies, the discovery of another record-setting loss from a rogue trader at a French bank and, of course, the subprime mess, the ratings process has never been under closer scrutiny. In its May 2008 release, S&P points out that changes in risk management practices in the financial services sector made as a result of the recent turmoil in the capital markets are expected to provide further learnings the agency can incorporate into its expectations of an effective ERM process in other sectors. With that said, the agency expects the fundamental structure of its ERM analytical framework to remain intact. The principal objective in evaluating ERM is to drive companies to implement practices that will limit the frequency and severity of losses that could potentially affect the ability of a company to repay its debt obligations on time.

The S&P RFC proposed to introduce ERM analysis into the corporate credit ratings for nonfinancial companies as a forward-looking, structured framework to evaluate management's overall capabilities, faithfulness in executing a sound strategy, and adaptability to a changing operating environment. S&P points out that "the quality of management judgment is not as easily benchmarked by quantitative metrics in the way that ratios and models of cash flow adequacy, liquidity, earnings capacity, and leverage [can be]." S&P's plan to benchmark companies against each other and over time ultimately will result in ERM analysis driving some rating and outlook changes.

S&P plans to eventually score companies to benchmark its opinions on ERM quality as one proxy for its assessment of management. The firm's purpose is to use the deterioration or improvement over time in a company's ERM quality to gauge rating and outlook changes before the consequences of extreme adverse events manifest in published

financial reports. S&P expects the value of ERM analysis “will be incremental in most cases, negligible in a few, and eye opening in some others.” In essence, S&P brings a creditor’s bias to evaluating a company’s ERM capabilities in a forward-looking manner, as evidenced by its comment that “a firm’s future ability to meet financial obligations in full and on time is more likely to be enhanced by strong ERM or diminished by weak or non-existent ERM.” The message is that rating agencies appear to be tying their historical sensitivity to significant and volatile unexpected losses to the rated entity’s ability to understand such volatility and prudently manage these risks through the application of ERM.

Recognizing that ERM is not a one-size-fits-all cookbook for all industries and that each company must tailor the ERM process to its specific circumstances, S&P’s November 2007 RFC proposed an evaluation framework based on the following analytic components: risk management culture and governance, risk controls, emerging risk preparation, and strategic risk management. The May 2008 release indicated that the agency decided to emphasize the two components most broadly comparable and critical of the original four areas included in the 2007 proposal – risk management culture and strategic risk management. The other two components were discarded for the time being. Beginning in the third quarter of 2008, S&P will incorporate the selected two components into its discussions with companies. This review process will entail information gathering, primarily, for the purpose of developing benchmarks. Scoring these two areas is unlikely to begin until sometime in 2009. Incorporation of the risk controls and emerging risk preparation components also is being deferred, with some specific exceptions.

Risk management culture

S&P seeks evidence that risk and risk management are important factors in day-to-day decision-making. The analyst will evaluate the organizational structure, as well as the roles and responsibilities, competence and accountabilities of the individuals who execute risk management. For example, he or she might inquire as to whether management has articulated the firm’s tolerance for risk, delineated the staff responsible for risk management, defined their reporting relationships, communicated the company’s measures of success, integrated risk management into performance management and budgeting, and clarified how metrics around risk management affect compensation.

Culture and governance are important because they are indicators as to the extent of integration and influence of risk management on corporate decision-making. A strong ERM process is one that makes risk transparent in corporate dialogue and communications up, down and across the organization by establishing risk tolerances and making them explicit in the execution of the business model. Compliance with regulatory standards is not enough. In fact, S&P states:

An excessive compliance culture may belie a weak risk management culture. This is because a compliance

approach to risk management usually means that the firm has neglected self-assessment and prioritization of risks and risk management activities, leaving those roles to the regulator.

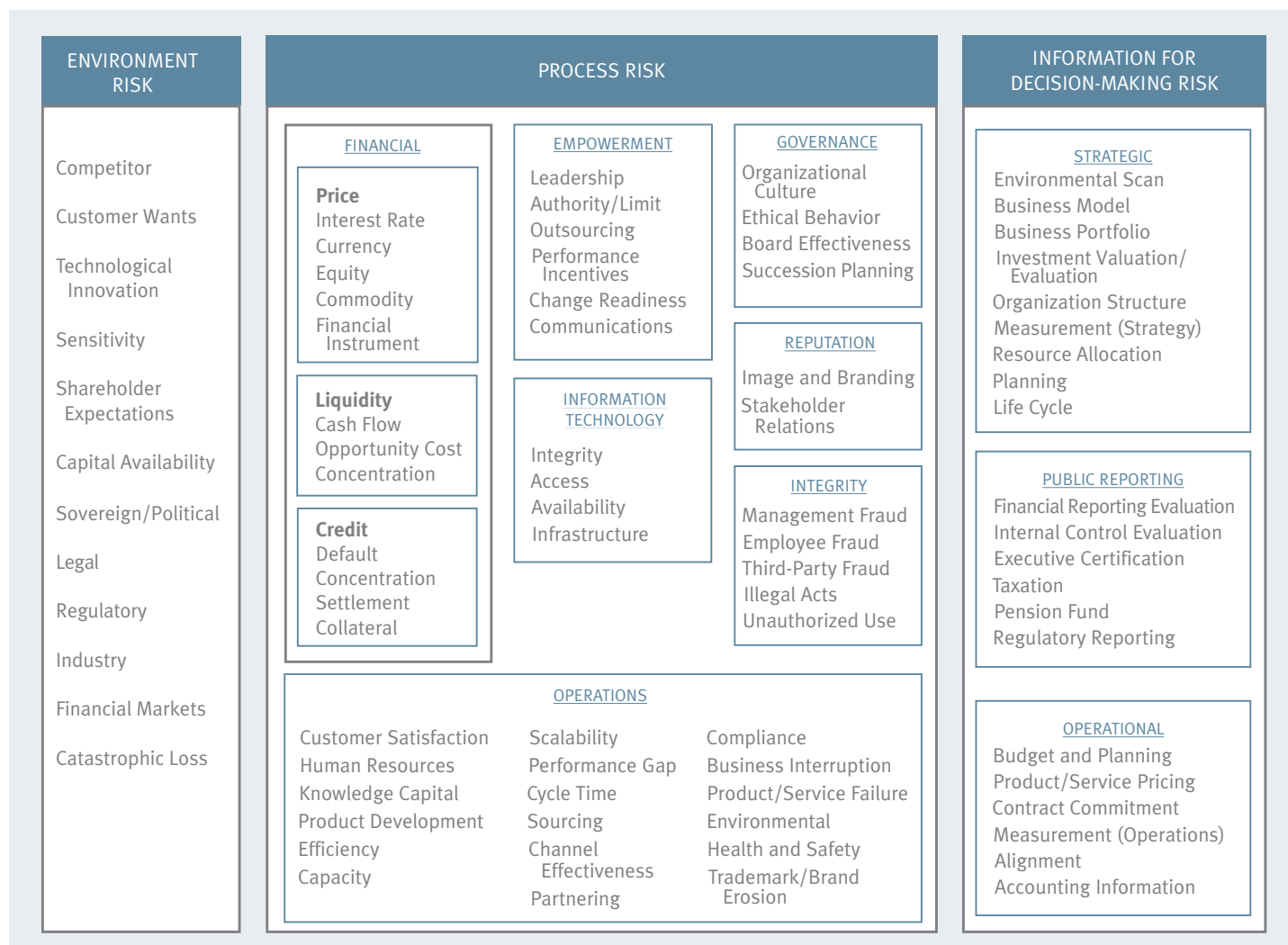
Strategic risk management

This component involves integration of risk, risk management and return for risk into the strategy-setting process. The analyst will focus on “understanding the firm’s risk profile, and obtaining management’s explanation of recent changes in the risk profile, as well as expected future modifications.” S&P states that the risk profile can be expressed in terms of earnings loss, impact on enterprise value, or through other financial metrics for various risks or for each operating unit. For example, the analyst might inquire as to whether the company uses risk/reward analysis when considering resource allocation decisions in strategic planning, making pricing decisions and measuring performance.

Strategic processes affected by risk and risk management capabilities include capital budgeting, business planning, performance measurement, product management, acquisitions and divestitures, new venture risk/reward standards, and incentive compensation, among others. S&P’s message is that the degree to which risk is a vital factor in managing these and other processes, and the degree to which the management of risk is a priority within these processes, are prime indicators of the quality of strategic risk management. While control of historic risks is important, the emphasis here is on a forward-looking analysis of potentially significant risk events that have not yet occurred.

In the RFC, S&P discloses its initial point of view of the key risks facing different sectors. For example, for oil and gas, S&P states the key risks include commodity prices, environmental concerns, natural disasters and weather, a pandemic, expropriation, and regulatory and legislative issues. For consumer products, the risks include failure to innovate, mergers and acquisitions (M&A) and restructuring, and reputation. For capital goods, engineering and construction, the risks include commodity prices, labor skills shortage, project management, strategic execution, liquidity, M&A and restructuring, and supply chain. There also are other nonfinancial industries for which S&P provides key risks, including airlines, automotive, chemicals, electric utilities, integrated gas, health products, health services, hotel and gaming, media and entertainment, natural resources, retail, technology and telecommunications.

In offering its point of view around key risks, S&P is granting insight as to the risks the rating service expects an organization within a given sector to be assessing, prioritizing and managing. Therefore, a company’s existing risk model needs to include these risks. For companies without a risk model, S&P’s list of risks is a good starting point for customizing one. S&P allows for management to consider other risks which, in effect, leads to a customized risk model by company.



To illustrate the potential risks to consider, we provide an example risk model above. This risk model depicts three groupings of risk – environment, process and information for decision-making. These risk groupings provide a broad foundation on which more specific categories of risk can be identified, and the risk categories within them can be customized by industry. The point is that companies need a common risk language with which to begin an enterprise risk assessment. Therefore, they should start with the key risks provided by S&P and add additional risks germane to the successful execution of the organization’s business strategy using examples in the above model.

For more information regarding the above risk model, we have provided a supplement to this issue of *The Bulletin* (see “The Protiviti Risk ModelSM – An Illustrative Risk Language” at www.protiviti.com).

Risk controls and emerging risk preparation

As part of its May 7, 2008, announcement of its ERM intentions for nonfinancial companies, S&P indicated that it is generally deferring the other two components of the review process – risk controls and emerging risk preparation. However,

where a single type of risk could result in a “material deterioration in credit (e.g., commodity price risk for an agribusiness company),” a more in-depth review of how that risk is managed and controlled will be conducted. Industries where this likely will be a focus include commodity-based sectors such as energy, utilities and agribusiness. These commodity-based risks can be measured, modeled and hedged, which enables S&P to apply a consistent approach that is within the realm of credit analysis tools it uses currently for financial institutions.

The RFC states that “firms achieve risk control through identifying, measuring, and monitoring risks, setting and enforcing risk limits, and managing risks to meet those limits through risk avoidance, risk transfer, risk offset, or other risk management processes.” If S&P drills down into risk controls in any specific area, it expects to see programs in place that manage exposures and losses within established limits, as well as drive “consistent execution ... so that future implementation will be a given.” S&P’s PIM approach will focus the analyst’s inquiry on:

- **Policies**, including business strategy, risk tolerances, risk authorities and disclosure requirements to be addressed through internal and external reporting.

- **Infrastructure**, including personnel, back-office operations, data and technology.
- **Methodology**, including risk metrics, stress testing, validation activities and performance measurement.

S&P points out that the relative importance of each of these areas to the rating service’s overall conclusion regarding risk control quality will depend on the complexity, size and risk tolerance of each company.

Similar to risk controls, another component – emerging risk preparation – is being deferred by S&P for now. However, aspects of this component may be relevant to the forward-looking perspective of strategic risk management. Risk management is not static; risk profiles constantly change. Recognizing this, S&P has defined emerging risks as “those that are completely new or extremely rare adverse events, and therefore cannot be managed via a control process.” Companies should deploy appropriate activities to anticipate adverse events and plan responses to them. These activities include “environmental scanning, trend analysis, stress testing, contingency planning, problem post-mortem, and risk transfer.” Depending on the nature of the business, the analyst may look (a) for evidence that a company is planning for extreme adverse events, as well as (b) for the results of such planning, both during and after the occurrence of such events. The analyst also might inquire about the company’s stress-testing practices and its contingency plans for extreme disasters.

What to expect next

Nonfinancials can expect questions regarding ERM relative to risk management culture and strategic risk management to be incorporated in their next round of ratings discussions with S&P analysts. These questions will be designed to allow S&P to develop industry benchmarks.

In the risk management culture area, S&P stated its analysts will focus on:

- Risk management frameworks or structures currently in use
- The roles of staff responsible for managing and reporting risk
- Internal and external risk management communications
- Broad policies and metrics for successful risk management
- The influence of risk management on budgeting and management compensation

Sample questions for risk management culture (as provided in a May 22, 2008, presentation by S&P executives):

- Do you have a risk management program?
- Is there a statement of risk appetite and/or tolerance?
- Which staff members are responsible?
- What are the reporting relationships?
- Which reports are seen by the CEO/audit committee/board?

- How do you measure success of the risk management program?
- How is risk management integrated into the performance and budgeting process?
- How do risk-related metrics impact manager compensation?

In the strategic risk management area, S&P indicated analysts would focus on:

- Management’s view of the most consequential risks the firm faces, their likelihood, and their potential effect on credit
- The frequency and nature of updating the list of top risks
- The influence of risk sensitivity on liability management and financing decisions
- The role of risk management in strategic decision-making

Sample questions for strategic risk management (as provided in the aforementioned May 22, 2008, S&P presentation):

- What are the company’s top five risks? How much revenue is tied to each?
- What is the likelihood and impact of their occurrence?
- What impact do these risks have on your cash management?
- How often are major risks reviewed to assess their importance?
- What strategic decisions have been affected by risk management and how?
- Tell us how a recent real risk was handled.

While S&P does not intend to perform an audit of management’s assertions in responding to the analyst’s questions, the agency has stated that it “will closely examine the consistency between their statements and historical performance.” The agency also notes that a discussion of ERM will become a regular part of its follow-up after significant drops in earnings or losses, significant restatements of prior financial statements, or material impairment losses and write-downs. The objective is to understand how managers have consciously taken and retained risks and why they are comfortable with their net risk positions. As noted earlier, nonfinancial companies operating in sectors where a single risk type has significant credit implications also can expect S&P to probe deeper into how that risk is managed, measured and monitored.

Some companies are prepared, others are not

The 2007 Protiviti U.S. Risk Barometer study (available at www.protiviti.com), which surveyed 150 senior-level executives from America’s largest companies, reports risk profiles are changing as America’s largest companies take on more risks. It also reports that risk levels, as well as appetites for risk, have changed significantly over the past two years. This is important from a rating service perspective, because increased vulnerability is a key indicator of the importance of ERM quality.

The Risk Barometer reports that just over half (53 percent) of organizations believe they are “very effective” at identifying

and managing all potentially significant risks. Using the survey data, we found that “very effective” companies are more likely than the other participating companies to:

- Deploy an enterprisewide risk management policy and a formal enterprisewide risk assessment process
- Implement a risk monitoring and reporting process
- Formally integrate the risk assessment process and the risk responses for key risks with business planning and strategy-setting activities
- Quantify risk to a greater extent
- Maintain an appropriate balance between the activities for controlling the business and the activities driving entrepreneurial and opportunity-seeking behavior

The message is that companies with more sophisticated risk management infrastructure are less ad hoc and more anticipatory in improving their risk management capabilities continuously and, therefore, will be more effective in avoiding surprises and keeping pace with changing risk profiles. Rating services are looking for precisely this.

Unfortunately, the Risk Barometer also noted that 47 percent of the participating companies were less likely to execute the above activities implemented by the “very effective” companies. These companies have work to do.

Where does your company stand?

If you are not sure how your ERM capabilities stack up, you should find out. Companies are advised to self-assess their ERM quality using the two S&P components to ascertain whether any gaps exist. Gaps should warrant careful analysis to develop action plans that improve risk management capabilities. While analysts bring the bias of a creditor to the ratings process (and therefore place a stronger emphasis on protecting enterprise value), the capabilities needed to address their concerns are a step in the right direction and will benefit shareholders as well.

The self-assessment diagnostic should focus on whether the company has the following:

- An enterprisewide view of risks and a process for identifying the priority risks, with an organized catalog of risks supported with definitions
- Policies and procedures in place for managing the priority risks that could affect the entity’s ability to pay its debt obligations in the future to within defined risk tolerances with clear ownership over, and accountability for, execution
- Demonstrated ability to avoid unexpected losses outside of established tolerance levels over time, with the objective of supporting a conclusion that the company is at least unlikely to experience such losses in the foreseeable future
- Clear evidence that risk and risk management capabilities are an integral part of strategy-setting and business plan-

ning, including the ability to relate key risk indicators (KRIs) to strategic objectives

A key objective for S&P appears to be reducing the *volatility* of losses. Accomplishing this objective requires a loss fact base in critical risk areas and ultimately sound modeling techniques and data-gathering and data-cleansing processes of both internal and external loss data. Otherwise, how can management know the risks are being managed? Therefore, earnings and cash flow volatility are likely to spark inquiries from the S&P analyst. Expect S&P to move in this direction in the future.

Some best practices for working with the analyst

With respect to the ERM inquiry itself, we recommend the following practices:

- **Involve your CEO.** Your top executive’s point of view as to the importance of ERM in managing the business is vital to the analyst’s understanding of ERM quality. It is important that the CEO support the objective of transparency and open communications around risk and risk management and be committed to a risk-sensitive culture. It is a safe bet that the analyst will be looking for this.
- **Articulate your risk profile from a creditor’s point of view.** While *enhancing* enterprise value is important and the risk-taking associated with opportunity-seeking behavior is a relevant and important topic, the analyst’s primary emphasis is likely to be on *protecting* enterprise value and balancing opportunity-seeking behavior with risks undertaken. Therefore, describing the company’s risk profile with a creditor’s bias toward reducing the risk of unexpected losses will help place into context the conversation around the importance of ERM quality. For example, if the company enters into complex transactions with complicated risks and is highly leveraged, the analyst or an S&P ratings committee may place greater weight on the ERM discussion.
- **Describe your process clearly.** The analyst will want to understand the company’s process for identifying, measuring, managing and monitoring risk. The analyst also may want to review descriptions of risk-control programs for priority risks that can be measured, modeled and hedged. In addition, he or she will want to note examples of execution. Your description of the process should address how it is integrated with the company’s strategy-setting and business-planning processes and how it impacts corporate decision-making. Be sure to describe how your policies, infrastructure and methodologies support your risk management culture.
- **Focus on what makes sense to your business.** The analyst will not expect the company to do everything exactly in accordance with the S&P criteria for ERM. The process is not a perfunctory “check-the-box” approach. The analyst will expect the company to vary its risk management capabilities according to its strategy, organizational structure, risk profile, risk tolerances and the complexity of specific priority

risks. Thus, be prepared to state the company's point of view around the what, who, why and how of risk management.

- **Recognize the bar will continue to rise.** At first glance, the S&P plan to hold discussions that will not impact the company's rating appears to be somewhat benign. In fact, S&P states that it does not expect "ERM analysis [to] radically [alter its] existing credit rating opinions." However, when nonfinancial companies experience unexpected losses, restate prior period financial results or face critical commodity or financial type risks, management should expect S&P's interest – and the stakes – to rise. As S&P benchmarks companies within a sector against one another, we can expect more specificity in the form of risk metrics, measurement tools and monitoring processes to emerge in specific areas as key differentiators. Finally, we do not believe that S&P has given up on scoring company ERM quality. It is just a matter of time. In its May 2008 release, the agency stated, "... we will develop benchmarks that will form the basis of scoring at some future date." The message is clear: The first

year under the approach outlined in the May 2008 release is only a beginning.

Summary

While S&P's approach is not as aggressive as contemplated under the November 2007 proposal and is focused on just two of the four categories originally proposed, nonfinancial companies should be prepared for the ERM-related dialogue with the S&P analyst. With the ever-changing operating environment, there has never been a better time for companies – financial and nonfinancial – to take a hard look at where their ERM practices stand. Once benchmarks are developed for different industries based on the agency's initial reviews in the first year or two, companies will be subject to comparisons against a standard. That comparison will be used to drive an assessment of management. Therefore, organizations with a high risk appetite, diverse businesses or complex risks should evaluate the need for improvements in their ERM infrastructure carefully.

Key Questions to Ask

Key questions for board members:

- Has management reported to the board on the status of the company's ERM process using the applicable rating service's evaluation criteria? For example:
 - Are the organization's risk management culture and governance functioning effectively? Is there sufficient clarity around the roles, responsibilities and accountabilities of those responsible for risk management, and are they positioned appropriately within the organization to influence corporate decision-making?
 - Do risk management policies cover such factors as risk tolerance, the company's internal and external reporting, and the processes, personnel and technology for assessing the critical financial and nonfinancial risk? Does the risk management infrastructure support risk communications at all levels?
 - Is risk management effectively integrated with strategy-setting and business planning?
 - Does the risk management methodology provide for appropriate metrics for assessing and quantifying significant measurable risks and incorporating risk into corporate decision-making?

Key questions for management:

- Have you self-assessed your company's ERM quality using the applicable rating service criteria (e.g., the S&P components) to ascertain whether any gaps exist? If gaps do exist, have you developed an action plan to improve risk management capabilities on a timely basis?
- Do you know what your priority risks are? Have you compared your list of risks against the key risks S&P identified for your industry in its November 2007 RFC? Have you considered emerging risks and your organization's ability to avoid losses in excess of established tolerances?
- Have you evaluated both the design and operating effectiveness of the policies, infrastructure and methodologies underlying your ERM process? If so, have you shared the results with the board?
- With respect to the priority risks, are they owned by someone or by some committee, function or unit empowered to act with clear accountability for results? Are these risks managed against established risk tolerances with the intent to reduce exposure to unexpected losses?

Need help preparing for the S&P credit ratings evaluation process? Whether you are identifying gaps, developing action plans to address known gaps or implementing remediation plans, Protiviti can help. We have worked with companies around the world to drive value from each step in this process. Call **1.888.556.7420** to speak with one of our Managing Directors regarding your ERM process and infrastructure or to learn more about the information covered in this issue of *The Bulletin* and what it means to your business.