Companies today face a broad array of risks—strategic, operational, currency, subprime, contract, customer, vendor, financial instrument, and hedging, to name a few. Hardly a day goes by without another business posting write-downs, recapitalizing, or seeking bankruptcy protection associated with poorly managed risks. What is enterprise risk management (ERM), and how are leading companies strategically managing risks to avoid being devastated by today's perilous marketplace?

STRATEGICALLY MANAGING RISK IN TODAY'S PERILOUS MARKETS

YOU NEED TO SUCCESSFULLY INTEGRATE STRATEGIC PLANNING AND ENTERPRISE RISK MANAGEMENT.

BY BOB PALADINO, CPA

In this article I'll explore the 2004 ERM framework (*Enterprise Risk Management—Integrated Framework*) of the Committee of Sponsoring Organizations of the Treadway Commission (COSO), which consists of eight interrelated components (see Figure 1). COSO defines ERM as: "A process effected by an entity's board of directors, management, and other personnel, applied in a strategic setting across the enterprise, designed to identify potential events that may affect the entity and manage risk within its risk appetite to provide reasonable assurance regarding the achievement of entity objectives."

I'll also review the practical application of the framework by The United Illuminating Company (UI), the company's integration of strategic planning and ERM, and the use of a process-based organization.

CASE: THE UNITED ILLUMINATING COMPANY

The United Illuminating Company, the principal subsidiary of UIL Holdings Corporation (NYSE: UIL), was formed in 1899 when the Bridgeport Electric Company merged with the New Haven Electric Company. UI is a regulated utility that delivers electricity and energy-related services to 320,000 customers in the greater New Haven and Bridgeport areas of Connecticut. Headquartered in New Haven, the company has more than 1,000 employees and revenue of $982 million. It also is the recipient of an APQC Best Practice Partner Award. (Recipients of this award are organizations identified by APQC as exhibiting exceptional performance or employing innovative approaches.) As a subject matter expert for this APQC ERP project award, I helped screen more than 50 leading organizations to arrive at just five that scored the highest on an ERM survey. UI was one of those five. These organizations served as the model for identifying and sharing best practices, and this article captures many of those findings.

Strategic Process-Based Management. UI employs a continuous strategic planning process to achieve strategic objectives, as shown in Figure 2. Edward J. Drew, UI associate vice president, strategic business services, states, "A defined, repeatable, and integrated governing process provides a basis for continuous improvement, shared knowledge, teamwork, and efficient use of executive time." Strategic objectives are typically long term, and progress is assessed and measured continuously to reflect gaps overcome and remaining, lessons learned, and changing business demands. These objectives are organized by four perspectives: financial, customer, operational, and capability. Projects to achieve these objectives are also defined through the strategic planning process, which includes risk identification and analysis. Annual goals are captured with a corporate balanced scorecard and balanced scorecards at the divisional levels, providing alignment across the organization.

ERM responsibilities are assigned to Strategic Business Services (SBS), the organizational unit responsible for the strategic planning process at UI. SBS reports directly to the CEO. This assignment enables UI to integrate ERM with strategic planning, process improvement, and project management—core practice areas of SBS—and to leverage process improvement and project management as risk management tools to increase the predictability of results. This effort results in an integrated strategic planning and risk management process. UI is a process-based organization (horizontal or cross-functional view), but it still uses a traditional vertical organization to manage budgets and staff (see Figure 3).

The process view reflects what the organization does as

Figure 1: COSO ERM Framework

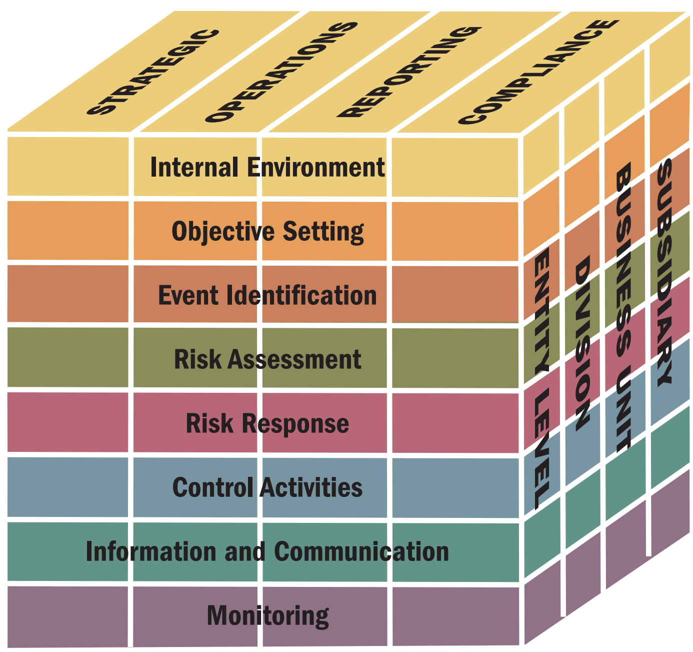


Figure 2: Integrated Strategic Planning and Risk Management Process

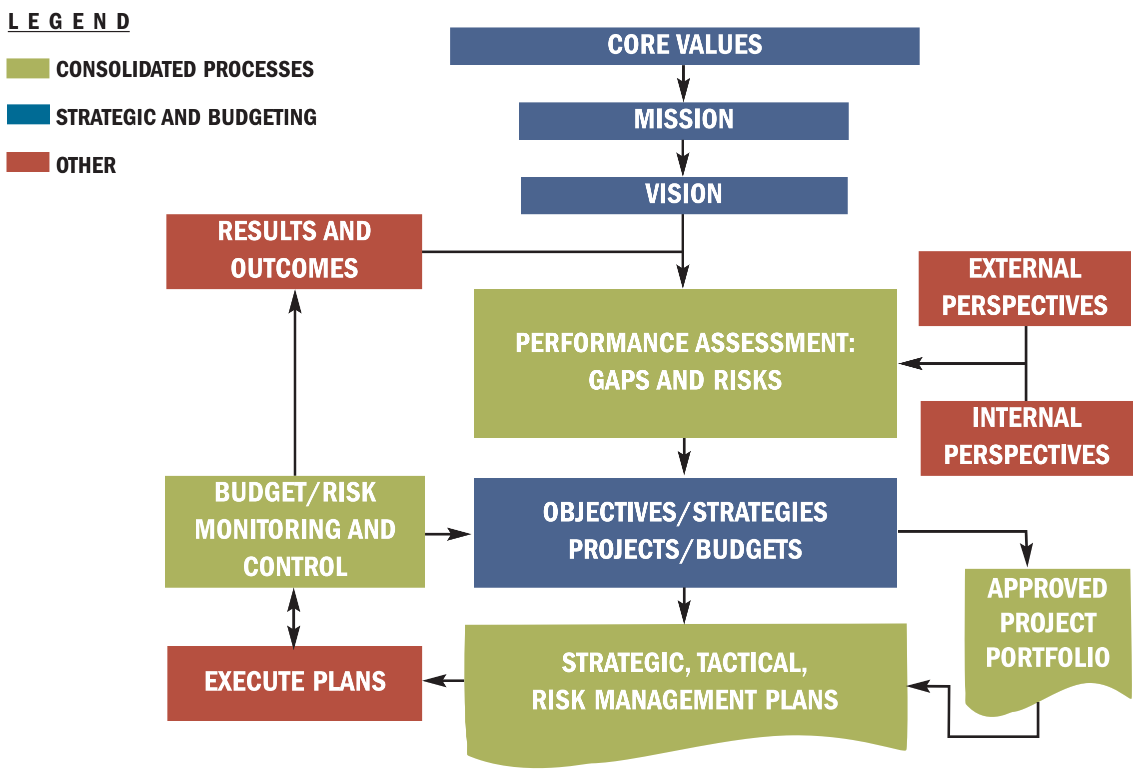
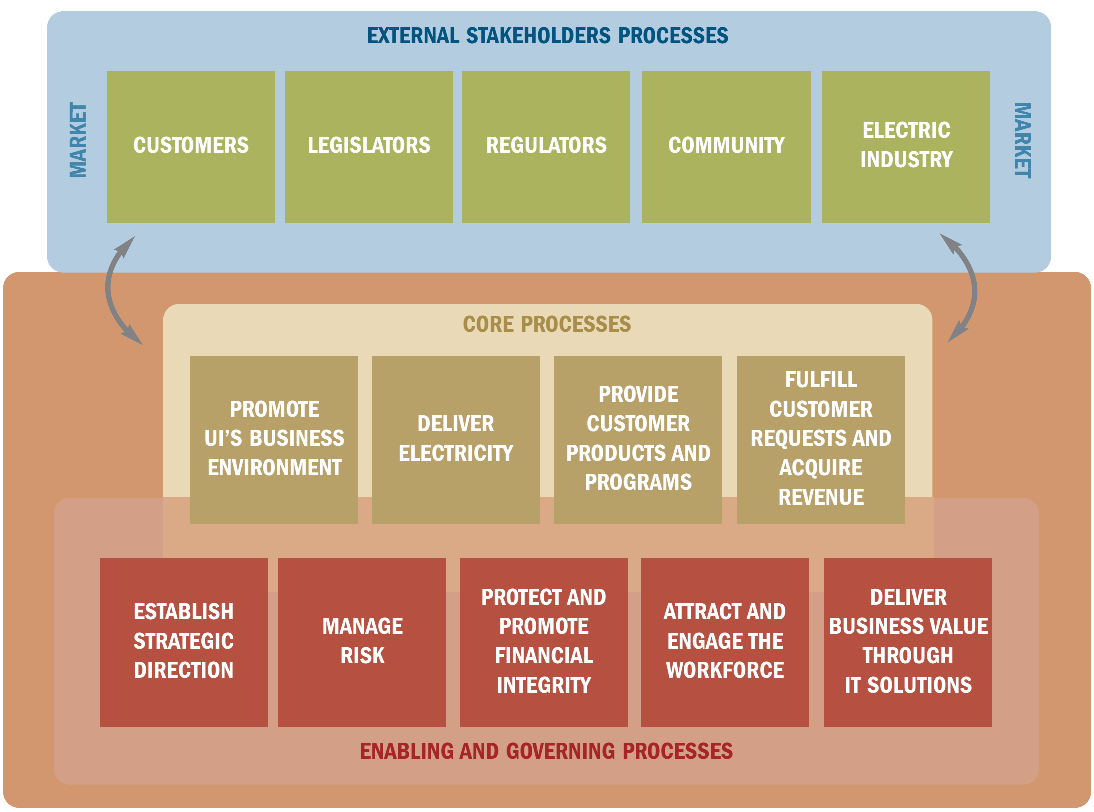


Figure 3: UI Process-Based Environment

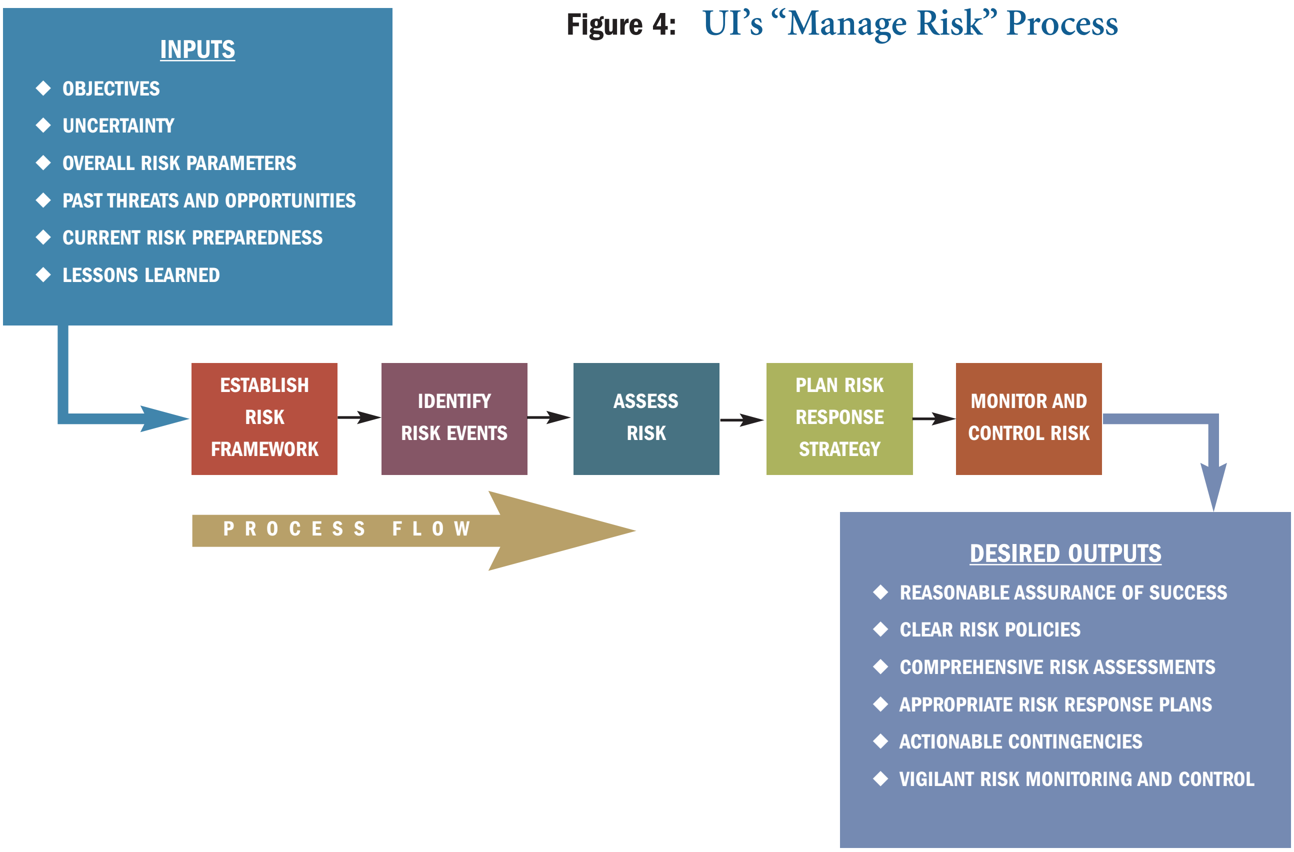


Risks can be either negative or positive, threats or opportunities. ***An opportunity not pursued can be a risk.***

a business, its core processes, and the enabling and governing processes necessary to be successful. As an indicator of the value the company places on enterprise risk management, "manage risk" is one of its enabling processes. Looking at risk from a process perspective offers advantages over a strict functional view. For instance, in addressing a risk with a functional boundary, the risk may get transferred to another part of the organization, which could have an overall negative impact on the organization. As an example, trespass and unauthorized entry into the company's electric facilities (such as an electrical substation) is a security and public health risk. The liability for this risk is insurable, so it resides in Finance's risk management function. Yet UI's process approach to such a risk recognizes that an effective risk-response strategy must involve "deliver electricity" because its personnel are responsible for maintaining and monitoring substation perimeter defenses, signage, and access control. The benefits of these risk management activities accrue to Finance (in the form of lower insurance premiums over time), but, even more importantly, they "promote UI's business environment" in the form of reduced reputational risks and an enhanced community safety record. The end-to-end perspective of a process is more holistic and allows more effective ERM.

SBS also prepares two major reports each year: one in October to evaluate the yearly Enterprise Risk Assessment (ERA) survey, used by the company's executives to reset the risk response strategies for the next year, and one in May as a major status checkpoint. These reports contain qualitative and quantitative data about identified risks and their associated strategies. They also include consid-

Figure 4: UI's "Manage Risk" Process



eration for regulatory (both state and federal), tax, legal, and industry changes that can impact the business.

UI's "Manage Risk" Process. Defining risk as one of UI's nine top-level business processes allowed the organization to focus on how risk is integrated with each of its other processes. The example above shows how the risk management process is integrated with "protect and promote UI's financial integrity," "deliver electricity," and "promote UI's business environment." Philip H. Turner, director, strategic planning and risk management, provides this insight: "Recognition of 'manage risk' as a top-level business process at UI provides visibility across the organization and indicates that managing risk is everyone's job, not just the CFO's or Audit's. This took an executive decision from our president and COO to effect. It also ensured that UI assesses how risk affects external stakeholder value rather than just internal measures." Using a blend of COSO and Project Management Institute (PMI) principles, UI established its "manage risk" process as shown in Figure 4.

This process has become the foundation for all of UI's risk activities, from strategic planning down to individual projects. The objective isn't to eliminate all risks but, rather, to manage them effectively. Risks can be either negative or positive, threats or opportunities. An opportunity not pursued can be a risk. For instance, an opportunity to preemptively replace aging components of the electric delivery infrastructure before device failure, if left unaddressed, could later result in widespread failures that can't be remedied quickly or cost effectively.

Central to this process is the concept that every manager is a risk manager. The expectation is that each manager within UI will:

- Be an expert regarding the risk events, likelihoods, impacts, and preparations required;
- Align the resources of the organization to continuously monitor and protect; and
- Apply the discipline of a well-defined "manage risk" process structure to provide reasonable assurance that UI can meet its objectives in his or her particular sphere of responsibility.

Although risk management wasn't new to UI, the company hadn't standardized it or applied it at all levels. Consequently, 14 special risk areas were identified (see Table 1).

Table 1: UI's 14 Special Risk Areas

SPECIAL RISK AREAS	RISK MANAGED
Safety	Injury/accident
Security	Crime/fire
Business continuity	Business interruption
IT disaster recovery	Widespread IT infrastructure damage
Storm recovery	Widespread energy service infrastructure damage
Claims	Insurable risks
Department of Public Utility Control review officer	Escalated customer complaints
Strategic planning	Strategic opportunities and threats
Project management	UI project portfolio risks
Process improvement	Process opportunities and threats
Environmental	Pollution/pollutants
Records management	Access/loss of UI records
Code of conduct	Fraud and reputational risks
Revenue integrity	Bills/theft of electric service

These were risk-response activities where a specific individual had already been assigned to proactively manage the risk, but the individual acted somewhat independently and without common language or process. The new process provided a consistent set of tools and terminology to more efficiently identify, assess, document, and manage risks with cross-organizational transparency and understanding of the tradeoffs. One result has been the promulgation of "manage risk" handbooks using a common template, each specialized to a particular risk area. The first-phase rollout of "manage risk" was targeted to these special risk areas.

To facilitate the rollout, owners of these special risk areas were asked to join a risk manager's forum, a learning community for sharing knowledge and working together. Many of these owners didn't realize that others within UI were doing similar things and had common needs and lessons learned that could be applied. In joining this forum, each owner was asked to:

- Formally adopt the "manage risk" process for their workflow in 2006;
- Help identify performance metrics focused on "measuring to improve" that could be adopted throughout the organization—for example, a common way to calculate value at risk;
- Record any process improvements in 2006, especially the dollar value of opportunities captured or threats reduced; and
- Use 2006 process measures to identify process gaps

UI's ERM approach is founded on ***literacy, accountability, and a proactive stance toward risk.***

and improvements to be targeted in 2007.

Another accomplishment of this group was to define a Common Investigative Policy for incidents that occur. Previously, each risk area had its own approach to investigations. While this worked, it made it difficult to build institutional knowledge, and staff who rarely were involved in an investigation needed to be educated for each one. The common investigative process helps provide a reference for everyone in the company and then is adapted to the unique needs based on the type of investigation.

In 2009, UI plans a focused rollout beyond the 14 specialized risk areas to further improve transparency, uniformity, and shared learning.

Ongoing ERM Management and Reporting. Communication of ERM is accomplished through a phased approach. The annual ERA survey exposes the organization to strategic risks that the leadership identified by asking managers to assess probability, risk, and preparedness. The participants also have an opportunity to identify risks that they believe senior leadership may have missed. The ERA report and subsequent Risk Action Plan to mitigate risk close the loop on this information and form the basis for projects and individual actions throughout the organization. UI wants everyone to be visible and involved. Additional communication occurs through leadership presentations and risk management training.

In order for the organization to participate more effectively in identifying and managing risks, UI conducts regular risk management training seminars. The primary vehicles for training are classroom instruction and one-to-one coaching. Introductory classroom instruction is generally delivered within the context of project management (when a new project team is assembled, for example), and UI's risk management course is extremely popular. UI also conducts mandatory process overview training for all new hires (in 2005, all existing employees were trained) that demonstrates how employees' jobs impact overall results and the importance of focusing on the overall results, not just a person's own job.

One-to-one coaching is usually offered by senior managers to their direct reports. This is essential for transferring knowledge, especially given an aging workforce—one of UI's strategic risks. Participation in the ERA also builds risk literacy across the workforce, and the risk managers' forum provides for peer review and a learning community.

The UI board of directors set a threshold for material risks to the organization that must be reported to them. In addition, UI has established the following characterizations for risks:

- "Very large" risks are those valued at more than $10 million.
- "Large" risks involve between $1 million and $10 million.
- "Medium" risks fall within a $100,000 to $1 million range.
- "Small" risks are those valued at less than $100,000.

These are guidelines for reporting risk within UI. Based on the characterization of the risk, it is elevated to the appropriate level based on signature authority levels. For example, "very large" risks get board of directors' attention; "large" risks are reported to division heads, etc. UI will typically avoid projects with risk levels disproportionate to their benefits, unless there are safety or compliance reasons to continue. But continuing in those circumstances requires additional and higher levels of approval and oversight. All types of risks within a project are quantified to a risk assessment and subjected to this scale. As an example, UI is currently constructing a new high-voltage transmission line. Associated with the approval for the project cost (approximately $200 million), risk impact and the probability of cost disallowance were quantified because cost recovery is a key risk, given that UI has to get regulatory approval to ensure 100% recovery. Mitigating that risk was part of the decision-making process before the project was authorized. UI is currently working to report aggregate risk assessments across the 14 special risk areas to UI's senior management. This is part of a goal to broaden reporting from a project-level view to a program or a portfolio view.

In terms of a more general benefit, these efforts have helped introduce risk management language into the company. Having this common language has enabled better articulation of the risks, thereby improving UI's ability to respond to them.

Ongoing ERM Measurement. UI uses the balanced scorecard and focuses measurement of risk in two ways: metrics of the "manage risk" process and effectiveness of how the business is being run. Dorothea Brennan, director of process improvement at UI, emphasizes, "UI's goals in this approach are to avoid process for process's sake and risk identification without associated response actions." The UI approach to metrics is founded on the following tenets:

- Start with and stay focused on what matters to customers, stakeholders, and regulators.
- Measure to improve; challenge people to state what they will do with a risk to improve the business.
- Don't measure just because a goal or risk was measured in the past or is easy to do.
- Include customer and supplier risks.
- Be careful to check for balance and to consider how people will change their behavior based on the metric—i.e., unintended consequences.
- Don't let the perfect be the enemy of the good. Or, as some companies say, keep it simple.

UI thinks of process in its broadest sense: Excellent process design includes what customers, other stakeholders, and suppliers/vendors do, not just what the organization does.

Historically, UI has measured many activities in its business using some end-to-end metrics such as reliability and customer satisfaction. It used literally hundreds of metrics. The new approach ties all metrics to processes so they can be actionable. In 2006, UI's balanced scorecard set goals for the development of metrics for all nine major processes and their subprocesses. This was achieved, and those metrics, with ongoing updates, are used throughout the company. Below are a few examples of measures created for "manage risk":

- Knowledge is measured by the percent of risk managers who formally implement the "manage risk" process, from surveys to handbooks to ongoing reporting.
- Defined results are measured by the percent of risk managers who implement an effectiveness measure.
- Monetized results are measured by the cumulative value of opportunities gained plus the value of threats reduced.

Defined results are used where monetized results aren't possible (reduction in customer complaints, avoided citations, accident rates, awards received, etc.). Monetized results include project portfolio return on investment (ROI), revenue recovered, and reduced losses from claims. Extending these results to the portfolio as a whole, you can get an overall ROI.

UI's ERM approach is founded on literacy, accountability, and a proactive stance toward risk. These are the organization's critical success factors. Awareness is a powerful tool because people who understand the company's approach tend to self-align. Ultimately, the most important gauge of success is whether UI achieves its short- and long-term objectives.

What's Ahead? UI has identified three lessons it learned in moving toward ERM:

1. ERM benefits from tight linkage to an organization's strategy-setting process.
2. ERM can be approached successfully from a process perspective.
3. A continuous improvement focus can lead to significant adoption of ERM best practices across ever-wider circles of organization personnel.

These are accompanied by their three best practices:

1. Exploit the natural links of ERM and strategy planning.
2. Unify ERM across multiple practice areas using a common process.
3. Be prepared to stay the course—ERM is a strategic initiative.

UI has come to understand that enterprise risk management is a journey. The organization has traveled far, has a clear road ahead, and intends to stay the course. ■

Special thanks to UI's Edward J. Drew, associate vice president, strategic business services; Philip H. Turner, director, strategic planning and risk management; and Dorothea Brennan, director, process improvement, for their fine contributions to this article and their participation in the APQC ERM project. Portions of this article have been adapted from their case study.

Bob E. Paladino, CPA, is the managing partner of Bob Paladino & Associates, LLC, and author of the book, Five Key Principles of Corporate Performance Management. *He is an advisor to boards of directors and executive teams, is a corporate speaker, and can be reached at bobpaladino@paladinoassociates.com.*