ENTERPRISE RISK MANAGEMENT IN PRACTICE

Profiles of Companies Building Effective ERM Programs

protiviti®
Independent Risk Consulting

Business Risk | Technology Risk | Internal Audit

TABLE OF CONTENTS

INTRODUCTION

Last year, Protiviti published *Guide to Enterprise Risk Management: Frequently Asked Questions*. That publication includes responses to more than 160 questions regarding many topics pertaining to enterprise risk management (ERM). One of its overriding themes is that ERM establishes the oversight, control and discipline to drive continuous improvement of an entity's risk management capabilities in a changing operating environment.

In addition, during 2006 and 2007, Protiviti interviewed executives from more than 20 companies to determine how their organizations were implementing ERM. We found that the insights gained from these interviews were useful in illustrating what companies were doing to set the foundation for an ERM implementation that accomplishes the objectives these organizations set out to achieve. Accordingly, we published most of these interviews on our KnowledgeLeader℠ website (**www.knowledgeleader.com**) for the benefit of our clients and colleagues who subscribe to that service.

As part of our ongoing Risk Barometer study, we have found that almost 50 percent of senior executives with 150 Fortune 2000 companies in the United States lack a high degree of confidence that their organizations' current risk management capabilities allow them to properly identify and manage all potentially significant business risks. In Europe, 70 percent of senior executives have a similar concern. The *2007 U.S. Risk Barometer* (available at **www.protiviti.com**) also indicated that top performing companies are more likely to utilize the following risk management best practices:

- Rigorously deploy a formal risk management policy, a formal risk assessment process and a risk monitoring and reporting process across the organization
- Formally integrate risk assessment processes and risk responses with the activities of the strategy-setting and business-planning processes
- Quantify their key risks and evaluate their risk profile
- Assign to a chief risk officer (or an equivalent executive) the primary responsibility for coordinating risk management policy, execution and reporting

These practices provide a foundation for ERM and are illustrated in the interviews we conducted during the last 18 months.

In light of the above, it made sense to us to compile examples of how different companies in the United States, Europe and Japan are improving their risk management capabilities. This led to our inaugural volume of *Enterprise Risk Management in Practice*, in which we have included a number of the profiles that we published on our KnowledgeLeader℠ site during 2006 and 2007.

In producing the various profiles for this publication, several common themes emerged that demonstrate why and how companies across multiple industries are improving their risk management capabilities:

- *External and internal change* often is acknowledged as a catalyst for implementing ERM. For the majority of the companies profiled, the ERM initiative was preceded by significant changes, such as: rapid growth; regulatory scrutiny; a highly publicized, unexpected loss; or structural changes in the industry.
- *Education and support* are fundamental to an effective ERM process. Consistently, the companies profiled highlighted the importance of laying a solid foundation for ERM by clearly defining,

communicating, validating and reinforcing the objectives expected to be achieved. Through this education and support process, the necessary buy-in is "earned" – a critical element of a sustainable ERM process.

- *Integration with key enterprise-level business processes* helps prevent ERM from becoming a separate and distinct appendage. By leveraging strategic and other business-planning activities and embedding ERM into those activities, ERM becomes a key element of decision-making – providing greater visibility into the most critical risks affecting the achievement of goals and presenting fact-based choices of how best to mitigate the risks. Some of our profiled companies also are striving to further integrate ERM into areas such as capital resource allocation, and merger and acquisition activity.
- *Alignment with company culture* underlies the successful ERM programs profiled. This alignment takes many forms in setting the foundation for ERM, including how accountability and ownership are established, whether and to what extent ERM resources are centralized, and the degree of flexibility given to business units in applying ERM methodologies and frameworks.
- *Defining the value of ERM* is a universal focus for all of the companies profiled. Some believe they can gain sustainable competitive advantage through effective ERM processes. Largely, this is attributed to clearly identifying the most critical hazard and upside risks, and making fact-based decisions on how best to mitigate the hazard risks and exploit the upside risks with the appropriate level of resources. It is also a result of maintaining accountability over executing the agreed upon actions. Other sources of value include breaking down silos in an organization to facilitate greater collaboration to develop robust risk management improvement actions, improved containment of the impact of risk events and incidents when they do occur, and enhanced communication of the most important risks and risk responses with key executives, senior management and the board of directors.

ERM continues to mature as a process, and organizations are finding many ways to implement practical ideas to continuously improve their risk management capabilities. As we have featured companies operating in different industries and countries, we believe you will find such ideas in each of the profiles in *Enterprise Risk Management in Practice* that can be customized to your own organization in your pursuit of ERM, whether you are just getting started or looking for ways to improve processes already in place. In addition, we encourage you to obtain a complimentary copy of our *Guide to Enterprise Risk Management: Frequently Asked Questions*. It is available at **www.protiviti.com**.

Protiviti Inc.
October 2007

Annual Revenues (as of 12/31/2006) – €13.8 Billion (Net)
Industry – Manufacturing (Healthcare Products)
Company Headquarters – The Netherlands
Number of Employees – 61,900

INTERNAL AND EXTERNAL FORCES SHAPE RISK MANAGEMENT AT AKZO NOBEL NV

A top-down approach to ERM coupled with a bottom-up methodology helps Akzo Nobel keep its vastly diverse business units aligned and focused on the same strategic vision.

Akzo Nobel nv, based in the Netherlands, is a global Fortune 500 company serving customers worldwide. The company's three segments – human and animal healthcare, coatings and chemicals – are subdivided into 13 business units, with operating subsidiaries in more than 80 countries. Akzo Nobel employs approximately 61,900 people and reported revenues for 2006 of €13.8 billion.

Since 2004, Dick Oude Alink has been Akzo Nobel's corporate risk manager, a newly created position for the company. Oude Alink leads Akzo Nobel Risk Management (ARM). Previously, he worked for ABN AMRO Bank as a finance, insurance and claims management specialist. He joined Akzo Nobel in 1992.

The diverse and decentralized business landscape at Akzo Nobel lent itself to the creation of a risk management function, according to Oude Alink. Each of the three business segments includes disparate business units. The pharmaceuticals business segment, dedicated to human and animal healthcare, includes three business units: Organon, an area active in gynecology, mental health and anesthesia; Intervet, the world's third largest supplier of veterinary products; and Nobilon, a startup group that explores opportunities for human vaccines.

The coatings segment comprises Decorative Coatings, which are products used by professionals and do-it-yourself enthusiasts; Industrial Finishes, including wood and coil coatings, specialty plastics coatings and adhesives; Powder Coatings (Akzo Nobel is the largest global manufacturer of powder coatings and world leader in powder coatings technology); Car Refinishes (the company is one of the world's leading suppliers of paint, services and software for the car repair, commercial vehicles and transportation markets); Marine and Protective Coatings, including paints and antifouling coatings for ships and yachts with the International® brand; and Nobilas, which manages the complete accident repair cycle of a vehicle, including the claims handling and invoicing of all parties concerned.

Finally, Akzo Nobel's chemical segment includes Base Chemicals, which is an important producer of chlor-alkali products in Western Europe and one of the leading salt producers in the world. This business segment also encompasses business units dedicated to supplying the world with Surfactants, Polymer Chemicals, Functional Chemicals, and Pulp and Paper Chemicals.

Four key drivers

While the company had control and auditing systems in place, it was confronted by four key drivers that drove it toward formalized risk management:

- Dynamic and complex business environment
- Changing risk arena
- Shareholder and stakeholder expectations
- Corporate governance requirements

The business environment at Akzo Nobel is dynamic and complex not only because of the vast diversity of its business units, but also due to other external factors. These factors include fluctuating exchange rates; increases in prices for raw materials and transportation; changing global regulations and meeting the needs of global customers; scarcity of resources; and the complexity of logistics involved in conducting business on a worldwide scale, particularly in emerging markets.

The changing risk arena at this international company, like many of its peers, showed a clear tendency toward intangible and non-insurable risks. These risks include loss of reputation, failure to adopt change efficiently and effectively, and failure to prepare for and respond to business interruption, as well as a host of risks related to product liability, environmental exposures, and computer theft and fraud.

Shareholder and stakeholder expectations and corporate governance regulations are intrinsically linked and are challenges familiar to most large global corporations. For Akzo Nobel, there are three elements that play a role in responsibility to shareholders and stakeholders: people, planet and profit. It is a critical mission for the company to be responsible to its customers and employees, the environment and shareholders. In terms of corporate governance, the company is dedicated to transparency in operations and risk-based thinking, and strives to be in full compliance with corporate governance regulations, such as Sarbanes-Oxley in the United States and Tabaksblat in the Netherlands.

First steps

"With these drivers in mind, we started on the business unit level to create risk workshops and action plans for our risk management initiative," says Oude Alink. "This gave us an entrance into the business. We made sure that we illustrated how enterprise risk management will help them in their management processes."

As the risk management initiative evolved, Oude Alink and his team drilled down even farther and worked directly with the company's manufacturing facilities. "We reached out to our management teams located around the world," he says. "From 2004 to the present, we have fully integrated risk management in our business groups and plant sites."

One of the primary components for the success is an annual meeting with business unit management in which Oude Alink and his team present risk management performance, showing management the progress their groups have made, as well as a forecast for work to come. "It is a personal approach that we find works quite well," he says.

Risk assessment

For Oude Alink, the most critical factor is the identification and accurate assessment of risks. "We want no surprises related to our finances, reputation, compliance initiatives or business principles," he says. "The way that we ensure against surprises is by bringing together the management teams responsible for certain areas in our organization and by exploring the scenarios that could affect their overall business objectives. With these scenarios on the table, we use an open, interactive voting tool that allows us to assess the impact of potential risks on those objectives. The results appear immediately on the screen for all to see, and in this way, we help facilitate a meaningful discussion around risk identification and assessment."

For Akzo Nobel, the benefits of risk management are varied. They include a clear and informed focus on business objectives and a prioritization of related risks. "Risk management is essential in that it clarifies our business objectives and our path for the future of the company," says Oude Alink.

Additionally, a structured risk management approach encourages the owners of different risks to come together and work toward a common goal. "When you bring them all together, they can achieve higher results," he says.

The risk management approach at Akzo Nobel is built on the following steps:

- Identification and classification of the business objective (strategic, operational or compliance)
- Management self-assessment, which includes a risk profile
- Risk response or action plans that correspond to each risk profile
- Risk consolidation, which depends on the interaction and collaboration among the business units and facilities
- Risk transparency, a detailed overview of the top 10 risks, and their risk responses

The most important challenge in adopting the risk management plan at Akzo Nobel was to obtain management support at all levels and to achieve the top-down approach, as well as the bottom-up methodology of reaching out to each business unit and facility. "Both approaches must work in tandem," Oude Alink says. "Successful risk management depends on the complete alignment of day-to-day business planning, reporting and management, as well as strategic vision." This is why he stresses the importance of the annual management meetings, to facilitate communication and maintain momentum from both ends of the management spectrum. "We created a risk management Knowledge Center at Akzo Nobel, so that our risk-related information is timely, accurate and readily available at all levels of the organization," he says.

The key success factors for the risk management plan are:

- Top-down approach and management endorsement
- Execution on all management levels
- Full alignment with business planning and reporting
- Bottom-up reporting
- Risk management workshop process as an integral part of management meetings
- Driver function on process and content
- Recognized Knowledge Center

Wish list

There are two items on Oude Alink's wish list. The first is to have a clearer, more transparent link of business risks and opportunities. "There is a need in our organization to bring that together in a much stronger way, to balance risks and opportunities," he says.

The second is to continue to demonstrate the need and the benefit for fully integrated risk management within Akzo Nobel. "We must continue to align our objectives, risk and controls by increasing transparency and providing assurance," he says. "Our objectives are changing all the time due to internal or external developments. Therefore, instead of fixed controls, we need to make them as flexible as possible so that we can truly manage risk. High risks need increased controls; lower risks require fewer controls. This type of dynamic risk management requires full transparency."

Annual Revenues (as of 12/31/2006) – US$3.4 Billion (Operating)

Industry – Energy

Company Headquarters – United States

Number of Employees – 5,151

ALLIANT ENERGY: RISK ASSESSMENT, COMMUNICATION ARE THE FOUNDATION OF ERM

To achieve a 360-degree view of risk and continually refresh its "risk universe," Alliant Energy relies on a team of dedicated staff responsible for administering ERM.

Alliant Energy is an energy holding company based in Madison, Wisconsin. Their domestic utilities, Interstate Power and Light Co. and Wisconsin Power and Light Co., provide power to nearly 1.4 million customers in Iowa, Wisconsin, Minnesota and Illinois. The company also maintains investments in the nonregulated generation arena, as well as in targeted international markets.

Joel Schmidt is the company's chief audit, ethics and compliance officer, in charge of overseeing the administration of Alliant's enterprisewide risk management (ERM) initiative. He is supported by a staff of dedicated employees focused on an ongoing collaboration with business unit functions. "The vice president of strategy and risk is the executive owner of this process," he says. "My team owns the administration of ERM, making sure the process exists and that it is validated. We have a staff of two – a manager and an analyst – both of whom have an extended network throughout Alliant, which helps us to create multiple links into the business. This is important because so much of the information we receive is qualitative, rather than quantitative. When dealing with qualitative feedback, it is critical to achieve a 360-degree perspective on risks and apply quantitative measures."

Beginning the initiative

Several key external factors created the incentive for Alliant to integrate ERM into the organization, including increased credit rating agency scrutiny on balance sheets in the aftermath of corporate governance scandals typified by the Enron debacle. "Additionally, underperformance of our nonregulated business units, and a general awareness of COSO within the industry groups, contributed to our growing recognition of a need for ERM," says Schmidt. "Internally, we began to question what went wrong and how we might have known earlier that we were at risk. This debriefing mentality began three years ago, and with it, the inception of a global ERM initiative."

Alliant embarked on the process by first conducting a cross-functional team review of Alliant's risk management and trading policies. "We then conducted a bottom-up survey of our risks," Schmidt says. "We worked with those close to the operations and verified and reviewed our findings with vice presidents and directors. Our process was to survey these individuals separately and as a group. Once the data was collected, the results were tabulated, prioritized and reviewed with senior management, and ultimately, with our Board."

The ERM team aggregates items into risk registers, which allow Alliant to track risks. After the risks are identified, they are taken through a quantitative and qualitative data analysis that measures operational, financial or other impacts. This process also includes identifying risk owners and assigning responsibility for mitigation strategies. In the end, the team identified 20 to 25 key risks, and assigned monitoring and mitigation accountability at the vice president level or above. Finally, the team developed monthly, quarterly and annual reporting mechanisms.

Risk assessment and reporting

One essential aspect of accountability, monitoring and reporting mechanisms is to ensure that Alliant's risk universe is continually refreshed. "At each meeting with the board of directors, we review the

corporate risk universe, highlighting new items and outlining significant changes," Schmidt says. "Additionally, on an annual basis, we put together a consolidated risk assessment that summarizes each top risk, including factors such as mitigation strategies, measurement tools and anything else that provides the context we need to effectively manage the risks."

Alliant's monthly outlook process is embedded into the financial forecasting process and includes reporting to senior management. In addition to participating in the outlook process, Alliant's vice president of strategy and risk discusses the risk universe with the board of directors approximately eight times per year. The business units are involved in both monthly and quarterly reporting, with an annual deep dive, in which the involvement of functional management varies depending on the issues facing the company.

Risk assessment is the foundation of an ERM process, according to Schmidt. "The most significant risk assessment tool we use is face time, getting in front of the business units on a regular basis to ensure that we understand the full context of the risk," he says. "Face time also helps foster an open environment for communication exchange. Other than this, we have kept our tools simple: spreadsheets, presentation software and databases. You have to assess the risks – their magnitude and their interplay with each other. Risk assessment is the root function for the whole process."

Benefits and challenges of ERM

The anticipated benefits to a comprehensive ERM program at Alliant include:

- Fewer mistakes
- Improved methodology for identifying issues before they spiral into significant problems
- Greater flexibility to align decision-making with organizational changes

The primary critical success factor, according to Schmidt, is the ability to integrate ERM into existing business processes. "This is a continual challenge," he says. "In our culture, it must be related to everything we do, as opposed to being an initiative that simply results in additional work for the field. To obtain buy-in from the organization, ERM must not be a discrete process, but rather, part of the DNA of the company. It's vital to listen to the front line and present ERM as a process that can solve real problems."

Embedding ERM into existing corporate practices can be a challenge. "If there is any way we can bolt ERM onto an existing process and use the information that is already being collected, then we will do so," Schmidt says. "We have made significant strides in embedding ERM into strategic planning, which is leading to strides in budgeting and, potentially, resource allocation. We have not made any inroads into mergers and acquisitions, but I believe ERM would be a strong tool for M&A in helping us understand how the cultures would meld together in the event of a merger. Thus, ERM could positively impact merger integration activities."

Schmidt's vision for ERM is that it will become part of Alliant's decision tool bag and provide boundaries for acceptable operating behavior. "ERM should be an enabler, not a roadblock, for organizational effectiveness," he says. This notion of setting boundaries is fundamental to keeping the organization focused, consistent with its business strategy and appetite for risk.

According to Schmidt, collaboration across the various business units will likely increase; the next level of maturity to emerge will be understanding the interrelationships of risks. "This will require a high level of collaboration, and we will need to ensure that there is a collective mechanism in place to avoid damaging enterprise risks. For example, a customer risk in one area may be tied to production risk in a generating plant, as well as a wire delivery risk. We must explore the summation of those risks, as opposed to looking at them as silo risks. The more complete the collaboration, the more robust a risk assessment process you will have. We are moving there, we are pointed in the right direction, but today, we have not achieved ideal collaboration."

Annual Revenues (as of 12/31/2006) – US$1.8 Billion (Net)

Industry – Manufacturing (Dental Supplies)

Company Headquarters – United States

Number of Employees – 8,500

ERM AS STRATEGY AT DENTSPLY INTERNATIONAL

For this global manufacturer of dental products, ERM is firmly linked with the company's overall strategic plan, as well as its Global Performance System.

DENTSPLY International provides the dental community with high-quality, cost-effective dental products. As the largest professional dental products company in the world, DENTSPLY operates facilities in 22 nations on six continents, distributing dental products in more than 100 countries under leading brand names in the dental industry. The dental profession looks to DENTSPLY to deliver innovative new products that advance the practice of dentistry.

Rachel McKinney, senior vice president of global human resources, has been with DENTSPLY since March 2003. In her current role, McKinney also helps lead the company's enterprise risk management (ERM) initiative, now completing its first year.

In mid-2005, DENTSPLY's board of directors agreed to explore ERM in order to gain a better understanding of the company's risks beyond the compliance and reporting needs that had emerged during work related to Sarbanes-Oxley. McKinney was asked to spearhead the effort.

"The first step was becoming more educated about the nature and scope of ERM," she says. "I wanted to make sure the entire executive team understood what ERM meant, so I conducted preliminary research of my own through networking and by exploring the Internet. Once we gained a better understanding, we realized we needed expertise to help provide a process." DENTSPLY engaged a consulting firm that specializes in risk management to help develop a common ERM foundation and establish a risk assessment process. The approach was to conduct an enterprise risk assessment and utilize the results to help incrementally establish an ERM infrastructure that was aligned with the company's strategic plan.

The first step of the risk assessment was the development of the DENTSPLY Risk Model, which included internal, external, strategic, operational and organizational risks. The risk model served as the foundation to provide a common understanding and perspective of the various types of risks inherent in DENTSPLY's strategy.

Leveraging the DENTSPLY Risk Model as a starting point, DENTSPLY developed and deployed an online risk identification survey to a core team of senior managers representing the company's worldwide divisions. Each online survey participant was asked to identify the top risks that represent barriers to DENTSPLY's strategic objectives. In addition, face-to-face interviews were conducted with key executives.

The results of the risk identification process served as the basis for a two-day executive workshop designed to further understand, evaluate and prioritize the core business risks in the context of the achievement of the strategic plan. During the workshop, participants discussed and evaluated each risk based on impact to the strategic plan, likelihood of occurrence and current management effectiveness. Based on the results of the risk assessment, 13 risks were identified as high priority and linked to corresponding strategic functions.

For each high-priority risk, the executive management team identified the risk owners to assume accountability to identify current processes and controls in place, as well as planned initiatives. "It was important at this stage to determine what we were already doing to manage the risks and then locate the gaps in our current operations," McKinney says. "Then, we developed the additional initiatives needed to close those gaps."

The strategic plan

Unlike some organizations that establish ERM as a separate function, with its own set of priorities, policies and action plans, DENTSPLY opted to link ERM to its strategic planning processes. "At the time, we were in the second year of our strategic plan that had been presented to and approved by the board of directors. We wanted to use the four objectives of that strategic plan as the basis for our risk assessment and core risk identification," says McKinney. "We gave ourselves an 18- to 24-month time frame to continue implementing the strategic plan and establish activities to mitigate risks associated with that plan."

The four objectives of DENTSPLY's strategic plan, supported by a wide range of specific actions and approaches, focused on financials, innovation, customer satisfaction and internal talent. ERM has been fully integrated into this plan and firmly linked to each of the four objectives. "As a result, there is really no end point to risk management," says McKinney. "We agreed to align our ERM efforts with our strategic plan, using core projects and processes to mitigate risks throughout the company. We see this as something that will continue to evolve and shape how we operate as an organization."

Another example of how risk management has been integrated into key corporate initiatives involved the rollout of a new global performance systems initiative. Last year, in its annual general senior management conference, the company introduced its Global Performance Systems (GPS). The impetus for GPS was the consensus among general managers and senior functional leaders to create more consistency around key processes to close performance gaps. "We identified key processes and their core risks," McKinney says. "For example, in the area of innovation, GPS highlights the risks related to technological innovation and product development and management, helping us understand those risks so that we can deliver on product development. We have to create consistent guidelines and build a program that can be rolled out to educate multiple functions around project management."

"With GPS and ERM, we are taking the core risks in conjunction with processes and initiatives and linking everything," McKinney continues. "In this way, ERM does not feel like something we are adding to our jobs; it has become the way we do our jobs. In some cases, the activity comes first and the risk fits in; and in other cases, the risk leads and the activity fits in. This is how we embed ERM into our business operations and strategy."

McKinney provides regular updates to the board of directors on the progress of the organization's strategic risk management work. Last December, DENTSPLY reviewed its strategic plan and the progress that had been made, examining current and planned activities. "As we design and implement solutions, the strategic plan evolves," says McKinney. "Last December, when we looked at our risks, we realized we were making headway on most points related to our plan. The goal is to make all of this the normal way the executive team operates and thinks."

The benefits of ERM

According to McKinney, this approach has helped create a more robust strategic plan for DENTSPLY. As the team implements strategies, they are focused on activities that will generate results associated with the plan. The approach also helps allocate scarce resources.

"Finite resources are always a challenge for us, as it is for most organizations," McKinney says. "One critical success factor is effective and consistent measurement. Whether you approach ERM as a discrete department or the way we approach it, you still have to keep your eye on the systems and process. You have to monitor the work in order to make any progress."

What truly differentiates the success of ERM for DENTSPLY is buy-in and a consensus from the board and senior management team. They understand and agree that in order for DENTSPLY to be successful in achieving its strategic goals, the company as a whole must proactively think about risks and integrate them into core processes.

Feedback from the company is generated through collaboration with specific projects targeted at particular risks, with five risk owners responsible for the 13 core risks reporting regularly on their progress. For the most part, however, ERM operates under the radar at DENTSPLY. "At a certain level of the organization, there is probably a cursory understanding that there is something called a risk management strategy and it involves several initiatives," says McKinney. "The bottom line is if you mention ERM to the general population here, they will not be familiar with it because we have embedded it into our work. We are simply providing directional guideposts around decision-making and allocating resources."

The evolution of ERM

DENTSPLY has made significant headway in some of its core risk areas, and McKinney sees an opportunity to recalibrate those risks. "We now have a chance to focus on other areas as we mitigate some of our original risks," she says. "We will recalibrate and take the team through the risk assessment process once again to target new or emerging risks, review our progress and move forward."

"It is sometimes difficult to determine the success of ERM," she says. "On a scale of one to 10, I would say we are a seven. The most important thing is to have executive support. The reason ERM is working at DENTSPLY is that our board has a high level of interest, and our CEO and COO see ERM as integral to achieving our business objectives."

Annual Revenues (as of 12/31/2006) – US$11.5 Billion (Net)

Industry – Energy

Company Headquarters – United States

Number of Employees – 13,739

THE ERM CULTURE AT FIRSTENERGY CORP.

FirstEnergy's evolving risk culture supports decision-making and resource allocation and helps confirm risk ownership in the business.

FirstEnergy Corp. is a diversified energy company headquartered in Akron, Ohio. Its subsidiaries and affiliates are involved in the generation, transmission and distribution of electricity, as well as energy management and other energy-related services. Its seven electric-utility companies comprise the nation's fifth largest investor-owned electric system, serving 4.5 million customers within 36,100 square miles of Ohio, Pennsylvania and New Jersey. FirstEnergy has $11.5 billion in annual revenues and approximately $31 billion in assets.

FirstEnergy was formed in 1997 through the merger of Ohio Edison Company and its subsidiary, Pennsylvania Power, and Centerior Energy Corp. and its Cleveland Electric Illuminating Company (CEI) and Toledo Edison Company subsidiaries. At the time of this merger, FirstEnergy doubled its size and became the 12th largest investor-owned electric system in the nation. In 2001, FirstEnergy doubled its size again when it merged with GPU Inc.

During the GPU merger, FirstEnergy decided to create a new management position to deal with the mounting complexities brought on by the company's rapid growth, as well as significant changes occurring in the industry: Deregulation was being discussed and negotiated with the state utility commission, and the organizational structure of the traditional utility entity was under scrutiny. Even more pressing was an event from the summer of 1998, when an active commodity market was beginning to gain visibility. During this period, Enron and other companies were engaged in online trading of power in the commodity market, a relatively new trend with regard to the buying and selling of derivatives. Most companies, including FirstEnergy, had no sophisticated credit tools in place to measure credit risk. As a result, FirstEnergy suffered a significant, and highly public, loss. This crisis drove the implementation of an enterprise risk management (ERM) initiative around the commodity operations at FirstEnergy and the creation of a risk policy committee.

Initial steps in the evolution of ERM

"While our vision was never to focus on speculative trading, we did have traders operating in the market, so an important initial step was to establish a robust set of policies, loss limits, value-at-risk limits and daily reporting with a risk team that checked every transaction," Kitty Dindo says. "We directed ERM at our commodities and sourcing group, and that focus continues today. It was the first step in our evolutionary ladder of ERM."

With the increased complexity of the organization, driven by the acquisition of GPU Inc., Dindo was named to the new position of Vice President – Chief Risk Officer (CRO). As CRO, it was Dindo's role to establish processes to manage risks well beyond commodities, reaching across the enterprise. Three groups report to her: the company's traditional insurance group, corporate credit division and ERM team. The first two groups existed previously in the company, but the ERM team was formed when Dindo was named CRO. Currently, it is staffed with seven professionals and indirectly reports to FirstEnergy's Risk Policy Committee. The Risk Policy Committee is a cross-functional group of company officers that began its role by focusing on risk management capabilities involving commodities. The committee then widened its focus to include broader risk issues.

"When the ERM group was formed, it was the equivalent of creating a whole new function," says Dindo. "Our objective has been to integrate risk management with our strategy and business planning process."

"FirstEnergy uses an integrated business planning process (IBPP) that is conducted annually with every business unit and support department. Within that process, the ERM group implemented a risk component composed of risk assessment tools and techniques," she says. "As business units design their objectives annually or over a three- to five-year time frame, we add a process to understand the risks that might impede those objectives."

To accomplish this, Dindo and her team conduct facilitated discussions and anonymous surveys with management of the company's business units. The discussions result in documented risk maps that plot risks according to significance and likelihood. The risks are then linked with action plans and risk owners. "This is our bottom-up approach," says Dindo. "It is conducted at the business unit level. One of our early goals was to give ERM visibility and credibility in the company; prior to this, ERM had been mostly conceptual in nature. With our involvement in IBPP, the company began to take ERM seriously and see its value."

Dindo uses a separate process to survey FirstEnergy's senior management twice each year. This represents a "top-down assessment" aimed at the entire enterprise, not just each business unit. The senior team evaluates how well risks are managed. The ERM group then correlates that input with the results from the individual business units. "It all comes together in many different ways," she says. "We produce various communication tools, facilitate cross-functional groups who debate and discuss the management of risks, and develop reporting tools and risks matrices. We have created a whole ERM culture that includes a specific risk language, assessments and methodology. Our goal is to establish a consistent point of view from the enterprise and business levels with regard to risk management."

Building an ERM culture

According to Dindo, the next step is to continue to improve the quality of information the ERM team produces to ensure that the organization, as a whole, recognizes its value and uses it consistently when analyzing risks and understanding options and decisions that can mitigate risk. "When I took this role, our CEO told me he wanted me to build a risk culture in the organization. Building that culture is one of the greatest benefits of ERM. It is a mindset. As each part of the organization assumes its area of responsibility, it is looking at the risk-reward balance of the decisions it is making. Management allocates resources with risk priorities in mind – the more significant and likely the risk, the more resources are allocated to mitigate it."

Another benefit Dindo notes is that ERM encourages collaborative thinking about risk. Risks do not exist in silos. They, and the activities that drive them, are often pervasive across an organization. Although many management experts outwardly eschew "silo mentality" in an organization, the fact is that most employees are managed within distinct functional areas. The ERM initiative at FirstEnergy has brought a fair amount of collaboration to the organization because of the cross-functional nature of risk management. While that is a "soft" benefit, it is nonetheless considered an important contribution by management.

One critical challenge Dindo faces is the difficulty in measuring the benefits of ERM. "When a risk is successfully avoided, it is hard to measure the value of the process," Dindo says. "Additionally, some risks, such as the impact of the aging workforce, are difficult to measure due to the nature of the risk. When risks defy measurement, they are far more challenging to manage." However, Dindo points out that most of the risks FirstEnergy faces, while significant, can be measured: fuel pricing, power pricing and interest rates, for example. Dindo and her team conduct extensive earnings-at-risk modeling on these risks based on historical trends and empirical data.

Another challenge is to make sure that the business units, not the ERM team, own the risks, and that business unit management adopts the appropriate risk assessment tools and approaches as part of their processes. "This is why it is an evolution," says Dindo. "When they take charge at the business unit level, we need to monitor the efficacy of the methodology and make sure the business units are measuring risks correctly and adopting the right mitigation strategies." In an ERM culture, business units should partner with the ERM team. Fortunately, collaboration is a strength at FirstEnergy; cross-functional teams work together with highly positive results.

How the ERM culture evolves

Dindo's vision of ERM is to develop better knowledge and information about FirstEnergy's enterprisewide risks, including the correlation between risks. "We want to be able to provide meaningful discussion and analysis to help us meet both our short- and long-term objectives," Dindo says. "We want to establish accountability and specific action plans to mitigate our risks.

"The goal is to make better management decisions and understand more clearly where the organization is going," she says. "To do this, it is critical to continue our culture of collaboration, so that the company can work together effectively and each business unit can work better on its own. We want to continue to strengthen our partnership."

Annual Revenues (as of 12/31/2006) – US$9.7 Billion (Net)
Industry – Hospitality/Gaming
Company Headquarters – United States
Number of Employees – 85,000

ERM AT HARRAH'S: A MARATHON, NOT A SPRINT

After merging with Caesars Entertainment, Inc., Harrah's integrated ERM as a way to eliminate the organization's "silo mentality" and create a more collaborative environment.

Harrah's Entertainment, Inc. is the world's largest provider of branded casino entertainment. Since its beginning in Reno, Nevada, 70 years ago, Harrah's has grown significantly through the development of new properties, expansions and acquisitions.

In the summer of 2005, Harrah's Entertainment merged with Caesars Entertainment, Inc. and grew from a $4.5 billion company employing 46,000 individuals to a $7.1 billion organization with approximately 80,000 employees. Today, Harrah's owns or manages 49 locations in 13 states and six countries, primarily under the Harrah's, Caesars and Horseshoe brand names. In addition, the company has properties under development in the Bahamas and Spain. With approximately 3 million square feet of casino space and more than 40,000 hotel rooms, the Harrah's portfolio is the most diverse in the worldwide gaming industry.

In the wake of such significant growth, it became crucial for Harrah's to prepare for the unique challenges and opportunities that arise during a period of unparalleled expansion. According to Lance J. Ewing, vice president of risk management at Harrah's, "Risk is a natural part of the gaming industry; it's part of our DNA. However, Harrah's had the foresight to integrate enterprise risk management into our organization to begin to rid ourselves of silo mentality and analyze risks on a holistic basis. As we incorporated this enterprisewide approach to risk, we recognized immediately that it is impossible for one department or division to fully own all of an organization's risks. We needed a collaborative approach."

First steps

"As we continue on our ERM initiative, we look at the many stakeholders who will be our collaborators. Enterprisewide risks affect all aspects of the organization – the ERM department may be ultimately in charge of ERM, but we need Harrah's stakeholders to work closely with the ERM team," Ewing says.

Since the risk management departments of Caesars and Harrah's were merged in June 2005, advances have been made to alleviate a silo mentality. Harrah's began the process of applying ERM to the organization by first evaluating what the company was doing right with respect to risk management. They examined Harrah's risk management foundation – insurance, claims and safety – and then the ERM leadership worked toward integrating compliance with Section 404 of Sarbanes-Oxley.

Now, when opportunities arise – for example, embarking on a new construction project or signing world-famous talent such as Celine Dion, Jerry Seinfeld or Elton John – the risk management team is brought in for consultation. "People are beginning to understand what enterprise risk means to them and how the overall ERM team can help allocate resources to mitigate significant risks," Ewing says.

"In addition to working with the vice chairman and chief financial officer on finance-related and compliance issues, ERM has a frequent dialogue with other C-Level officers on broader risk management issues and themes when needed," Ewing says. "We also have the support of the general counsel and

chief litigation officer, who we work with on ERM-related issues including claims, contracts and liability issues. ERM works with the audit committee, and champions Sarbanes-Oxley and 404-related issues. ERM works with the treasury department on lines of credit and bonds, and the overall work of building a basis for understanding how, why and when we are spending money."

"The risk management team has an open door policy: Anyone can use our resources and our services. We stand ready to help to move people from making decisions based on gut instincts to making decisions based on sound knowledge and information," he says.

The ERM marathon

Identifying and assigning risk management roles across the enterprise begins with a comprehensive risk assessment. Ewing and the ERM team evaluate a wide range of internal risks, from terrorist threats to entering overseas markets. "We brainstorm the 'what-ifs,'" he says. "We have to make sure the squeeze is worth the juice. In other words, we calculate the upside and the downside of the risk and the reward."

At Harrah's, risk management helps to: (1) identify risk and reward, (2) determine the worst- and best-case scenarios, and (3) develop a business risk-response plan for assessing and responding to the identified risks. The risk management department uses a wide range of tools for this assessment and response, including risk modeling, actuarial science, forensic accounting and insurance brokerage expertise, as well as external auditors and other third-party providers. "Our support network is great both outside and inside the organization," Ewing says.

According to Ewing, the key benefit of an ERM approach is the enhanced ability to use knowledge and information for optimal decision-making. "We are in our late freshman year in ERM," he says. "We are still feeling our way through, and next year, we will have much more experience. The merger with Caesars Entertainment brings more risk-related resources to Harrah's, which we plan to leverage to sharpen the ERM focus. As we continue implementing ERM strategies throughout our organization, we anticipate reductions in claims and risks, more educated business decisions and a greater return on investments. The results are not immediate. ERM should be viewed as a marathon, not a sprint."

Facing challenges

The most significant challenge that organizations face when implementing an ERM initiative is defining and producing performance measurements. According to Ewing, it is crucial to have both short- and long-term goals and measurements in place. One important measurement that Harrah's is working to establish is ensuring that the ERM philosophy and methodology is communicated to all the departments and divisions, so that the risk management department is brought in on all relevant projects.

"I don't think that risk management professionals have always had a seat at the table," Ewing says. "That chair is being held out for us now, and our challenge is getting to the table in a timely fashion, providing effective resources and making meaningful assessments."

With this in mind, critical success factors going forward will include:

- Delivering resources effectively and efficiently;
- Crafting an appropriate response in a timely manner; and
- Demonstrating return on investment.

To date, ERM has been embedded in key business processes within Harrah's. For example:

- Strategic sourcing (purchasing) embraced a risk management focus, with Ewing's team ensuring that transactions with suppliers and vendors are conducted with regulatory and financial integrity.
- The mergers and acquisitions function now involves the risk management department in major transactions, such as acquisitions of both the Imperial Palace in Las Vegas (purchased in December 2005) and the Barbary Coast (purchased in 2007). Ewing and his team were included early in the process, giving them the opportunity to fully understand and respond to the specific exposures the acquisition created.
- The strategic planning process has set aside a budget covering both enterprise and traditional risk management.

Since ERM is being incorporated gradually at the corporate level into several core processes, the risk management department has identified the property management function as its next greatest opportunity. "We have work to do in the field," he says. "Part of our objectives and measurables will be to make sure that the right risk decisions are made at the property level."

"ERM needs to be the fabric of our decision-making as a corporation," says Ewing. "When decisions arise, we will be making them based on the information and the knowledge we glean from our ERM processes. The future of ERM for Harrah's is identifying the leadership within and outside the company that can provide us the resources to make sound business decisions, while mitigating our relevant risks and exposure."

Annual Revenues (as of 12/31/2006) – 24.0 Billion Swiss Francs (Net)
Industry – Manufacturing (Cement)
Company Headquarters – Switzerland
Number of Employees – 90,000

AN EVOLUTION OF BUSINESS RISK MANAGEMENT AT HOLCIM LTD

Holcim sustains and refines its business risk management (BRM) process with two key tools – a Risk Map and a Risk Driver Mind Map – which provide a holistic view of risk.

Holcim Ltd is one of the world's leading suppliers of cement and aggregates (crushed stone, sand and gravel), as well as further activities, such as ready-mix concrete and asphalt including services. The Group holds majority and minority interests in more than 70 countries on all continents, and employs some 90,000 people.

Business Risk Management

Six years ago, Holcim embarked on a Business Risk Management (BRM) process – a systematic and proactive way of looking at risks and opportunities.

Today, Clemens Mann* is the risk manager in the Department for Corporate Strategy and Risk Management at Holcim. In this role, Mann is responsible for ensuring that all the elements of the BRM process are in place, including methodology implementation and execution, database maintenance, risk champion training, and compiling and preparation of the corporate risk report. Looking back to why the company embarked on this BRM process, Mann points out that many of the factors that existed then are still present. "The changing of the business environment was a very important point then, as it is now," he says. "The internationalization and globalization of the cement industry, which migrated from a national industry towards an international business of global and regional players, was and is a key driver for us. Increased competition, stricter environmental and business regulations, greater accountability for the board of directors, and finally, the growth of our company all led to an awareness of a need for BRM. Those factors still exist today."

First steps

Implementing BRM began with a pilot phase in 1998. At the close of 1999, Holcim conducted a groupwide launch and rollout for BRM, starting with its largest and most significant business segment, cement. In 1999 and 2000, the implementation expanded to all companies of the group, with the BRM core team conducting risk workshops within various group companies.

Holcim's BRM process consists of six steps. The first three are to identify, source and measure risks, and the second three steps are to evaluate, manage and monitor risks. According to Mann, the benefits of integrating risk management into the strategy and business planning process have been proved, because otherwise BRM would be a standalone process and, as such, lose much of its efficacy and impact. "It is an ongoing challenge to achieve this integration," he says.

Holcim's business planning process is structured along three main phases:

1. Strategy Assessment
2. Strategy Development
3. Business Plan

The first phase of the process involves risk assessment, which integrates the first three BRM steps of identifying, sourcing and measuring risks. "In this first element of the business planning process, we

*Since this profile's original publication in 2006, Mr. Mann has left Holcim Ltd.

look at the risk profile in each of our group companies and examine how the business environment has changed or might change in the future," says Mann.

"To develop a truly comprehensive risk profile, we analyze both internal and external risk factors to determine where to focus the business planning process and where the critical elements reside. This way, we know where and how to dig deeper," he says. "From this actual risk profile, we make preliminary decisions about our future or so-called 'target risk profile,' and this results in the first indications of how we want to handle the risks." According to Mann, measurement or the quantification of risks is always a challenge; improvement in this area requires continuous reviewing of past assessments and gathering future information.

The second phase is strategy development, which integrates the BRM step of evaluating risk. For example, if a group company identifies the risk of increased cement imports into its markets, it develops and evaluates strategic options for how to handle that risk. Possible solutions might be improving product quality, enhancing customer relations or expanding technical services. "You go from issue to issue, and finally this gives us the strategy," says Mann.

The third phase is setting up the business plan, which integrates the final two BRM steps of managing and monitoring risk. This phase relies on resources, which are always limited, making it important to balance the different priorities in the region and in the group, in order to agree on action steps and objectives. "At the end of this phase, we have our functional plans, which are the outcomes of the business plan that describes not only the detailed strategy – meaning, what we seek to accomplish – but also, how to achieve that strategy, with specific actions for separate functions, such as marketing and sales, production or finance," he says.

In 2000, Holcim launched a Lotus Notes database to house critical information and improve the speed and accuracy of information exchange. At that time, the risk assessment process was also extended to other business segments like ready-mix, aggregates or concrete products.

"We also extended the BRM process to large projects throughout the company, such as building a new cement plant or entering a new country," says Mann. "We implemented our approach on a case-by-case basis for projects, and on an annual basis for the ongoing activities of our group companies."

In 2003, Holcim introduced a Web-enabled database called the BRM Tool to enhance standardization of the information housed in the Lotus Notes database and facilitate the analysis of the data. "Today BRM is fairly well implemented in our company," says Mann. "People have a good common understanding about risk management."

Risk tools

Two primary tools help to sustain the momentum and success of Holcim's BRM initiative. The most prominent is the Risk Map, which provides a good overview and visualization of the company's risk profile. Holcim's Risk Map is segregated into four quadrants. On the map, the X axis depicts the likelihood of a risk or opportunity, and the Y axis illustrates its potential financial impact or significance. It is used to develop actual and targeted risk profiles during the business planning process.

The second tool is the Risk Driver Mind Map, which is a visualization not only of the various risk sources, but also their relation to each other. "The Risk Driver Mind Map allows us to fully analyze the risk," says Mann. "It is an effective discussion tool that we use in our risk workshops to delve into the drivers behind the identified risks. The Risk Driver Mind Map is supported by a complete description of the risk situation from the workshop discussion." This tool provides the means of sourcing risks to understand where, how and why they exist.

These tools help Holcim with one of the most pressing challenges companies face in an enterprise-wide risk management project: the issue of quantification. Mann says that, in his experience, some of Holcim's group companies go quite deep in the quantification of risk, while others do it to a lesser extent. Holcim does not use Monte Carlo Simulations or other quantifying models, but rather, conducts this measurement on a simple basis. "For us, it's the prioritization of the risks based on what is

important to the company, the relative positioning of the risk on the Risk Map," he says. This positioning helps drive the focus of formulating appropriate risk responses.

Soft and hard benefits

The key benefits of Holcim's BRM initiative include both soft and hard results. Soft results include increased risk awareness, better change management, faster learning and, importantly, enhanced upward communication. For example, by integrating risk assessment with the business planning process, and by using risk workshops both in routine business operations and special projects, communication has improved. "Last year, a group company embarked on a $1 billion project," Mann recalls. "We gathered the management team together to conduct a risk workshop about the project, with representatives from all departments like production, marketing and sales, logistics, finance, HR, legal and others. This allowed us to gain a comprehensive viewpoint of the risks involved with this significant project. It is extremely valuable to compare views and insights across the company."

The hard benefits, like the issue of quantification, are more difficult to convey. "One indicator for me is lower cost of capital through investor confidence," says Mann. "Recently, Holcim has been acknowledged as leader of the industry in the Dow Jones Sustainability Index. Many initiatives within Holcim were measured as part of that rating, including BRM. For me, this represents a certain measurable benefit or, at least, an acknowledgement of the efficacy of our enterprisewide risk management process."

Lessons learned

Mann has two pieces of advice for anyone beginning an enterprisewide risk management initiative. The first is to obtain firm and visible support from top management. "If management is not convinced that it is working, then it will be easy for the business units to shift attention to other priorities," he says. "At Holcim, top management fully supported BRM, and this was a key factor in our success."

The second lesson is to focus on the content and not on the process. "For such a global, diversified company like Holcim, it is important to keep the business risk management process simple but solid," Mann says. "There is a latent danger to let the process grow and expand in many different directions, picking up more and more issues along the way. By keeping it simple and straightforward, but giving also a certain flexibility, it will be much more accepted by the line management of the various group companies. One way to accomplish this is to critically review the process and the results from time to time, and to keep the administrative work involved in the reporting process as minimal as possible; for example, by using an easy-to-manage IT tool."

Mann also points out that piloting the program with a few group companies proved beneficial because it allowed the rest of the organization to better understand and anticipate BRM. The feedback received from the pilot companies has been integrated, assuring that the final users contributed to the process. Piloting resulted in worthwhile enhancements to the process and achieved both executive management's and the board of directors' confidence.

"It is also important to achieve a consolidated view about the risk profile of the whole company," says Mann. "You must bring together the whole picture of the company from different regions and different business elements like marketing, technology, finance and other areas to set the right priorities. This is the essence of an enterprisewide point of view. Analyzing risks and opportunities for collaboration on common business issues, such as clustering our facilities, balancing capacity utilization, bundling purchasing power and creating shared IT service centers, have given us the opportunity to truly benefit from that collaboration."

"It is critical to remember that you are focusing on the whole enterprise," Mann adds. "By aligning the view on business risks of the board of directors, executive management and group companies, you will achieve greater levels of success and improvement, not only in the ongoing business operations, but also in special projects, such as mergers and acquisitions. For me, that is the value of enterprisewide risk management."

Annual Revenues (as of 12/31/2006) – US$3.1 Billion (Operating)
Industry – Energy
Company Headquarters – United States
Number of Employees – 4,440

THE EVOLUTION OF ERM AT MIRANT CORPORATION

The energy company emerged from bankruptcy with the help of its established risk management practices, and went forward to evolve those practices into a comprehensive ERM initiative, creating a culture of risk awareness and positive change.

Mirant Corporation is an independent power company that generates and sells electricity for customers in the United States, the Philippines and the Caribbean. As a power company, Mirant manages risk as part of its business model.

Paul Sobel has been the vice president of internal audit for Mirant for the past three years. His colleague, Anne Cleary, is Mirant's vice president and chief risk officer, a position she has held for about one year. According to Sobel, while it was broadly believed that Mirant had leading-edge risk management capabilities, it also was acknowledged that these capabilities were in pockets or silos throughout the organization. "Once we emerged from bankruptcy, the time was right to leverage our existing risk management capabilities and practices, which had been put in place over time, and expand them across the enterprise," he says. "It is important to note that without those existing risk management practices, we may never have emerged from bankruptcy; so, they were a good place to start."

Led by Cleary and supported by the internal audit (IA) team, the first step was to brief Mirant's newly formed audit committee on how the company approaches risk. This was accomplished during audit committee orientation, conducted just before Mirant came out of bankruptcy. The next step was to update Mirant's Business Risk Profile, a key enabler for enterprise risk management (ERM).

"Our Business Risk Profile represents a compilation of the risks facing the company, all of which have been assessed, based on a five-point scale, for residual impact and likelihood," says Sobel. "From there, risks are classified into four buckets: major, key, moderate and minor. The intention is to provide formal updates to the audit committee or the board of directors on the status of all 'major' risks."

Inherent and residual risk

"Coming into a new year out of bankruptcy was a two-step process," Sobel says. "We needed to develop a full-year audit plan and justify that plan to the audit committee by creating a risk universe. Due to the timing of my audit committee presentation, I took the first step of developing a risk model based on inherent risk to support my audit plan. This was an important first step. Anne took the second step of facilitating meetings with management to transition my risk model to become Mirant's Business Risk Profile, which was focused on residual risk. Anne presented our updated Business Risk Profile to the audit committee in May 2006, and it was well received. Traditionally, our Business Risk Profile had outlined key risks and tactical actions, but it lacked a robust point of view and focused mostly on strategic and industry risks. We took a big step this year to include inherent risk and residual risk, creating a comprehensive risk universe that has been assessed based on impact and likelihood criteria."

According to Cleary, it's important to examine inherent risks when looking at the audit landscape. "You can't assume the controls work, so you need to first look at the inherent risk and then analyze the residual risks, determining where you have the greatest potential breakdown of controls, and organize your work in that way," she says. Cleary approached the Business Risk Profiles based on the concepts put forth by the COSO ERM model. She wanted to achieve value, not just documentation. "I wondered how to get that value add out of having looked at the risks of the company," she says. "I started with the more residual risks because I was trying to identify where we could make improvements, create economies of scale and scope, and break down silos."

As an example, Cleary cites Mirant's risk control function. "Compliance and risk control have common skill sets and intersections for accomplishing their tasks. We recently made inroads to link the two, so that legal compliance and risk control do not operate in silos, but are instead brought together – which, in an international operation, is proving to be very useful."

According to Cleary, Mirant has three components in its ERM approach that contribute significantly to its success:

- A robust risk management policy
- A risk oversight committee (ROC) that meets on a regular basis and covers appropriate risk topics
- Risk management monitoring and reporting capabilities that go beyond global risk assessment

The risk management policy

Mirant's policy focuses on four key aspects of risk management: how market risk is to be monitored; how various models are to be used; how elements of operational risk are to be managed; and how credit risk is to be dealt with.

Market risk. "We focus our market risk efforts in places where we have merchant revenue gross margin exposures," says Cleary. "We are focused primarily on the U.S.-based business, because our overseas businesses don't have the same characteristics. They are more price-regulated."

Model oversight. "This deals with the necessary controls for the models that calculate the exposures of Mirant's market risks," she says. "The inputs to the model, as well as their core logic, have tight controls around them. For example, if someone wants to change a specific characteristic on how one of our generating plants is modeled, these controls govern how input is signed off on and change is allowed."

Operational risk. "This portion of our policy examines how we ensure that we have complete and accurate representations of deals, as well as how we check the mark-to-market activities for our portfolios, validating the commodity curves we use," she says. "This is the section where we outline how reports are to be submitted, who must report, and how and when we can change the reporting structure. If a control is changed or violated in any way, reports go to the risk oversight committee and beyond."

Credit risk. "Finally, we examine how we will grant credit and calculate exposures, both potential and actual, to counterparties," she says. "We determine how we will track activity in the event of a change of counterparty status, codifying that so that it is under the purview of the risk oversight committee. We also include management of our collateral requirements in this area."

All controls and activities surrounding those controls are reported on a periodic basis to management, the risk oversight committee and the audit committee. "Across all four areas, we have reporting requirements," says Sobel. "In the event a control is broken, specific remediation and reporting requirements are outlined."

The ROC

Senior Mirant management comprise an ROC that meets monthly to review reports from various risk areas across the company, including market and commodity pricing trends, legal compliance, insurance, environmental health and safety (EH&S), and regulatory. For example, under the direction of the ROC, there are a number of daily, weekly and monthly reports that are produced by the risk control function to report the status of the trading operation to senior management. Additionally, business units report in from the field regarding operational performance and EH&S.

"Our audit committee chartered the management-level ROC, a group responsible for not only the risks related to the areas the members manage, but also for coming together and assessing the risk activities across Mirant," Sobel says. "From a governance perspective, this has a high profile. It's where everything starts."

"As I examine risk management methods at other companies, I have come to understand that the greatest risk is not that the company is unaware of its exposures, but that only portions of the company are aware," he says. "When this happens, factions within the company may work at cross purposes. The ROC is our vetting arena. All risks come through this group, which ensures enterprisewide awareness and engenders open discussion in this innovative forum."

Monitoring and reporting

Mirant's risk management policy defines the controls and reporting that are required at a minimum. "We report more than the policy requires," says Cleary. "We have a series of daily reports to management that come out of our operational trading controls area. We segregate errors from violations. For example, somebody may perform a task improperly, but that does not mean the policy has been violated. This is an important distinction: If you track errors along with violations, you gather more complete data. Even when someone does not violate a policy, the error is still a problem for the organization. Inadvertently inaccurate information, while it does not create a violation, does get caught in our downstream process. The risk control function tracks whether or not the error showed up, where it emerged and how long it took before we caught it. In this way, we examine trends in errors and look for ways to improve."

ERM has been embedded into Mirant's resource allocation, but is somewhat informal relative to the other practices. Cleary and Sobel are now looking at further integrating risk controls, compliance and internal controls resources and toolsets to create better economies of scale and scope across the risk control and compliance universe. This will continue to reinforce the emphasis of risk on a global basis across all functions. "We believe ERM will be more formally integrated into strategic planning as our new management team moves forward with the updated Business Risk Profile," says Sobel.

Risk assessment continues to play a critical role in Mirant's ERM initiatives. "With regard to our enterprise risk assessment, Anne has facilitated meetings with business people who have opinions and insights regarding critical risks," Sobel says. "This was a collaborative effort that helped us reach agreement with regard to the level of residual risk in the company. Risk assessment is not limited to the CRO and the IA team discussing risks. It is a truly inclusive process."

Continuing the journey

Sobel says that his vision for ERM at Mirant is that it will be so thoroughly embedded in the culture and the way people think that it will be viewed less as a program or initiative and more as simply an operating and management style. "While we plan for incremental improvements to the program, we feel we are past the initiative stage and moving toward this vision," he says.

According to Cleary, she is hoping to further leverage the work accomplished to date. "In the past three to four years, our emphasis has been on risk controls for our merchant generation group and, like all U.S. businesses, we also had to focus on Sarbanes-Oxley compliance. Now we are integrating administration of legal compliance into our risk control framework. We are hoping to build on what our Sarbanes-Oxley team has achieved – namely, the development of effective tools for the acceleration of issues. We want to institutionalize those achievements, so that they become more a part of the fabric for the company."

Sobel adds, "The risk mindset has pretty much been embedded in our culture. The key is that we have taken a first and important step of recognizing the whole array of risks that Mirant faces and making sure the key risks are truly being managed. When we get to the next layers of risk, we will gradually roll out responsibilities for management and reporting. Importantly, the structure of the ERM program is in place, and outside of ongoing continuous improvement, I don't see any significant changes that would be needed."

Annual Revenues (as of 12/31/2006) – US$6.2 Billion (Net)
Industry – Consumer Products
Company Headquarters – United States
Number of Employees – 23,500

COMMUNICATING THE REWARD OF RISK MANAGEMENT AT NEWELL RUBBERMAID INC.

For Newell Rubbermaid, the first step toward integrating its risk management initiative was educating management and others on how the process differs from operational excellence.

Newell Rubbermaid Inc. is a global marketer of consumer and commercial products with 2006 sales of approximately $6 billion and a strong portfolio of brands, including Sharpie®, Paper Mate®, DYMO®, EXPO®, Waterman®, Parker®, Rolodex®, IRWIN®, LENOX®, BernzOmatic®, Rubbermaid®, Graco®, Calphalon® and Goody®. The company is headquartered in Atlanta, Georgia, and has approximately 23,500 employees worldwide.

As a decentralized organization in 2005, Newell Rubbermaid's decision to embark on a risk management initiative designed to span the organization relied on two key components: education and communication.

Bob Busch is the vice president of internal audit at Newell Rubbermaid and a proponent of risk management across the organization. "Our definition of risk is the chance of something happening that could significantly enhance or impede our ability to achieve current or future business objectives," Busch says. He and one auditor from an internal audit (IA) team of 20 work on the risk management effort, drawing support and collaboration from the company's business line management, as well as the corporate functions, such as legal and treasury, that focus on traditional, contractual and insurable risks, such as currency and commodities.

The structure of the company has played a role in the way risk management is implemented at Newell Rubbermaid. The company breaks its total business into three global operating groups, each with a designated group president and group CFO. Within those groups, the company has 23 business units or divisions, each with its own division president and division CFO. For the purposes of risk management, the corporate CFO asked the group presidents and CFOs to identify their top five to seven risks per division and outline how those risks would likely impact the achievement of current and future business objectives.

To accomplish this, each division quantified the estimated range of annual impact for each risk according to two quantitative measures – net sales and operating income. The divisions ranked the likelihood of each risk on a high, medium and low scale, and then estimated both impact and likelihood for the next three years. "Due to our decentralized operating structure, the impact is not viewed on an enterprisewide basis, but rather, tailored to each division and then rolled up. A division's risk that seems relatively low today on a quantitative basis may become more significant over time," Busch says.

The initial risk management effort proposed roles for both the business units and corporate. The business unit roles include:

- Identifying, prioritizing and quantifying downside risk (and upside reward) to the business
- Putting mitigation plans in place for downside risks
- Collecting and reporting the data to be aggregated at corporate

The proposed corporate roles include:

- Approving the overall risk management policies and guidelines
- Providing technical expertise and support for operations in areas such as legal matters, financial reporting and foreign exchange hedging
- Standardizing tools and templates and sharing best practices with business units
- Embedding risk considerations into existing processes, such as strategic planning, budgeting and business reviews
- Aggregating business unit exposures
- Communicating key risks and mitigation strategies to the board of directors, rating agencies and investors

"In June 2005, we communicated our risk definition, objectives and proposed roles to the groups, and asked the division and group presidents and CFOs to embed risk in their strategic planning process for 2006," Busch says.

Why risk management?

Busch admits that Newell Rubbermaid does not embrace the concept of "enterprisewide" risk management. The decentralized nature of the organization initially resists centralized initiatives. Yet, the concept of a comprehensive risk management approach has met with initial success at the company. "There were two primary external factors that moved us in this direction," says Busch. "One was the New York Stock Exchange (NYSE) listing requirement that audit committees review the risk management processes of the company, which includes examining how the company identifies and prioritizes risks and takes steps to mitigate exposure to risks." The second factor was Sarbanes-Oxley, which requires larger publicly held companies to include an internal control report that contains management's assertions regarding the effectiveness of the company's internal control structure and procedures over financial reporting. Part of that internal control structure includes five components of internal controls:

- Control environment
- Risk assessment
- Control activities
- Information and communication
- Monitoring

These factors emerged for Newell Rubbermaid in July 2002 with the Sarbanes-Oxley Act and in November 2003 with the NYSE listing requirement. By May 2004, a practical application of these factors was communicated internally in an initial external business risk profile for peer consumer product manufacturers. The profile was based on Form 10-K and proxy disclosures, and was intended to promote an industry-level discussion with regard to risk-based activity and related disclosures.

"We were asking the divisions and groups if the IA function was focused on the most significant business risks, while ramping up activities to comply with Year One Sarbanes-Oxley requirements," he says. "At the same time, senior management recognized the importance of this risk-related point of view. In the summer of 2005, business units were asked to identify both their business risks and their plans to mitigate those risks."

Integrating risk management

The first step in integrating risk management at Newell Rubbermaid was to educate managers, directors, select vice presidents and CFOs on how risk management is different than operational excellence. "Leadership wanted to understand how and why risk management was different than

just running the company well," Busch says. In response, 10 questions were identified through secondary research. These questions are called Key Decisions Guiding Risk Management Activities:

1. How do I define "risk" at my company?
2. How do I prioritize risks at my company?
3. Do I need to implement a formal enterprise risk management (ERM) framework?
4. Why isn't everyone pursuing a comprehensive risk management program?
5. Which works better: a centralized or decentralized approach to risk management?
6. What role should the corporate center play in risk management, versus the line?
7. How should I staff/resource my risk management program?
8. How can I embed risk management into existing business processes?
9. How can I convince the line of the value of risk management and drive change?
10. What information should I provide to my board/audit committee?

After guiding management through the responses to these questions, the CFO and his staff collaborated to solidify the direction and purpose of the risk management effort. "We also used external information to show what other companies were doing in the context of risk," says Busch. "The list of 10 questions was a core component of our education program and helped the leadership become comfortable allocating time to the risk management effort."

The second step in integrating risk management was relevancy. "Now that everyone understood the nature of risk management, it was time to explain its relevancy to the company," Busch says. The COSO II model was used to depict strategic, operational, legal, compliance and financial risks in light of the market capitalization decline drivers for the top 20 percent of the Fortune 1000. The most significant decline drivers from strategic exposures, such as poor acquisition or merger integration, decline in core product demand and competitor infringement on core market. "We then explained that the most significant drops in market capitalization stemmed from unmanaged strategic risks," he says.

To the extent that high-priority risks are identified, mitigation plans are assigned at both the business unit and/or at the corporate level, as appropriate. Certain risks, such as those surrounding foreign currency and commodities, require action plans assigned centrally. Other risks, for example, those related to customer service, are assigned to business divisions.

The risk management difference

All of this led back to the original question from leadership: What makes risk management different from good management?

"Risk management is different in two ways," says Busch. "First, you have to agree on an approach integrated with corporate strategy that outlines exposures, issues and problem areas. Second, you have to review and monitor the plan and make adjustments to it as needed. We already had quarterly business reviews in place, which, due to the short duration, do not allow us to get to the specific root causes of variation from the plan – a key indicator that a potential unmanaged exposure exists.

"Risk management is different than traditional management because it allows us to examine what is missing in our routine business process, and why those missing elements expose us to risk," Busch continues. "Risk management encourages better up-front planning and allows us to determine if our policies and capabilities are well aligned to the strategy we desire to execute. It also facilitates post evaluations to help assure improvements actually occur as intended."

Newell Rubbermaid is moving forward and including risk identification in its strategic planning process. In a November 2005 meeting, they discussed the aggregate risks that span the enterprise and common mitigation plans. "We now know what needs to be done on a process level to facilitate improvements in each of the three groups we started with. We will begin discussion on Newell Rubbermaid's appetite for risk and risk tolerance, as the understanding improves how risk management is integrated within good management," Busch states.

Risk management challenges and rewards

Busch anticipates that three key benefits will be derived from the comprehensive risk management program: a proven anticipation of outcomes, better resource and capital allocation, and improved budgeting.

The challenges are somewhat more complex. Communication is essential for gaining support and understanding about risk management. "Our challenge is to help the person who hears about risk management or enterprise risk management for the first time to truly understand that it is not a fad, and that it can represent a way to accelerate significant performance improvement," Busch says. "We are validating the business case for risk management through effective, continuous communication and interaction with business units. This allows us to manage the operating exposures at the source."

The company's critical success factors for risk management include gaining widening support for risk management and achieving visibility in the strategic planning process. Beyond that, the vision is to more fully integrate risk management with strategic planning, budgeting and capital allocation, refreshed quarterly through business reviews. "We have agreed that the best thing to do going forward is to embed risk management into our company's existing business processes," he says.

Panasonic

Annual Revenues (as of 3/31/2007) – ¥9.1 Billion (Net)
Industry – Electronics
Company Headquarters – Japan
Number of Employees – 334,402

SEEING THE POSSIBILITIES: THE JOURNEY OF ERM AT PANASONIC

At the root of this global electronics manufacturer's modern ERM initiative is its founder's early 20th century management philosophy.

Panasonic was founded in 1918 by Konosuke Matsushita as Matsushita Electric Industrial Co., Ltd. Today, with more than 600 companies, it is one of the largest electronic product manufacturers in the world. Panasonic manufactures and markets more than 15,000 products under well-known brands, such as Panasonic, National, Technics and Quasar.

Panasonic's internal structure is based on 14 business domain companies, each with its own distinct research and development, production and sales divisions. These divisions respond to their own business segments, such as AV, home appliances, industrial solutions, and other electronic and consumer products.

According to Yuki Miyazaki, the general manager of Panasonic's corporate risk management office, the company embarked on an enterprise risk management (ERM) initiative in 2005. Four key factors led Panasonic to adopt ERM. The first was Sarbanes-Oxley: Since the company is listed on the New York Stock Exchange, it had to comply with Sarbanes-Oxley requirements. To prepare for this, Panasonic took a unified and comprehensive risk assessment approach, which had been missing in the company.

The second factor was the frequent occurrence of problems related to product quality and liability, and information security. "We realized we needed to strengthen management-level activity to combat these problems," Miyazaki says.

At this point, the company's leaders looked back to the management philosophy of Panasonic's founder, Konosuke Matsushita. In the 1920s, he wrote a philosophy that focused on accountability and learning as the core values of management. Today's Panasonic team realized that those concepts represented important reasons to strive for an effective ERM program within the organization.

"Our founder's philosophy has much to do with risk management," Miyazaki says. "Konosuke Matsushita said that the cause of the failure stays always in ourselves, or in our own company. If a person complains about a failure, and says that it is due to another person or environment, such a person cannot learn from the failure. If a person thinks of himself as his own cause of failure, he may learn from it and may eliminate the cause of failure in advance. Then, he will never fail to succeed in his business whatever the business environment will be."

Konosuke Matsushita also advised his colleagues to be aware of signs of change within the environment. "The untrapped mind is open enough to see many possibilities," he said.

Finally, the fourth factor that contributed to Panasonic establishing an ERM initiative was the necessity to achieve a critical and challenging business goal of global excellence by 2010, which includes 10 percent profit and ¥10 billion (Japanese Yen) in sales turnover. "To achieve this, we must stretch to reach a higher target and reduce risks," says Miyazaki.

The first steps

Panasonic established its Global and Group (G&G) Risk Management Committee, consisting of nine directors in charge of special functions, such as environmental and product liability. Miyazaki's corporate risk management office acts as the secretariat of the G&G Risk Management committee. "Similar

risk management committees were set up in all of our 39 business domains," he says. "Once this was accomplished, we rolled out our G&G risk management assessment."

The assessment includes a list of 40 identified standard risks that may exist throughout the company, and it corresponds to a risk assessment questionnaire. These materials are distributed to all business domains worldwide. Miyazaki's team collected the results and then asked each of Panasonic's headquarter business functions to evaluate the findings and include their own insights and information.

Measurement

Miyazaki and his team measure risk, in part, in terms of financial impact – a rating of "super-high" represents a risk of more than ¥10 billion; "high" is between ¥1 billion and ¥10 billion; "medium" is between ¥100,000 million and ¥1 billion; and "low" is less than ¥100,000 million. Additionally, four core elements are evaluated:

1. Stockholder viewpoint
2. Brand and social trust
3. Human lives (safety)
4. Compliance

As for the likelihood of occurrence, Panasonic has three levels: high, medium and low. "High" means a once or more per year occurrence; "medium" is between once in 10 years to once annually; and "low" means less than once every 10 years.

Implementation

At present, ERM implementation centers around two components – risk and business risk. *Risks* are unpredictable factors or events that could impede business goals and must be covered by risk assessments. *Business risks* are unpredictable factors or events that could impede the promotion of business policies, plans and strategies. Miyazaki and his team conduct an annual review of business risks to strengthen the business plan and help secure management's goals.

The links between ERM and Panasonic's business plans are clear: First, each of the company's 39 domains' head offices collect information from their divisions and analyze and consolidate that input. Each domain reports these risk assessment results to headquarters by mid-December. "Business risks are discussed during meetings in March each year to foster a shared understanding of risk and an understanding of how to take specific measures against risks and their scope of impact," Miyazaki says.

In early December 2007, the Accounting Division of the Head Quarter will make an announcement to formulate its business plan, with the intended result being that business domains will fully embed risk assessment as part of their business plan.

Anticipated benefits

According to Miyazaki, there are four primary benefits to the ERM approach that Panasonic has adopted:

- The company's corporate strategy and action plan can be realized more easily by eliminating impeding factors.
- ERM prevents unacceptable events or situations that could prove to be harmful to the company, thereby reducing potential losses.
- Panasonic's business domains will be better prepared to manage new risks that might emerge due to changes in the business environment.
- The company's business plan and financial targets can be enhanced through the effective use of ERM.

"It is a challenge to persuade senior management, including the management in the business domains, of the benefits of ERM," Miyazaki says. "A critical component of our success has been our founder's philosophy. After studying this philosophy and incorporating it into our ERM philosophy as the basis of our risk management activities, we even produced a book this year titled *Learn from the Risk Management Philosophy of Our Founder Konosuke Matsushita*. With this guidance, we have been able to shift our company's culture toward embedding ERM into existing strategies, such as our midterm and one-year business plans. In the midterm business plan, each business domain has to measure risks within and outside the domain, and design countermeasures for these risks, for the period [from] 2007 to 2009."

A vision of the future

As Konosuke Matsushita writes in his passage, *The Way:*

Every person has a path to follow.
It widens, narrows, climbs and descends.
There are times of desperate wanderings.
But with courageous perseverance and
personal conviction,
the right road will be found.
This is what brings real joy.

Miyazaki and his team are continuing on the path toward achieving a successful integration of ERM at Panasonic. "We have tremendous collaboration and cooperation among our business domains," Miyazaki says. "For instance, soon we will be introducing a risk management workshop. We will hold a seminar in early September [2007] for 140 individuals throughout the domains and from various functions of the Head Quarter. Once these seminars are completed, we can proceed with our workshops, in which a facilitator will oversee ERM processes, including the identification of risks, the selection of major risks, and the analysis of the cause and structure of risks."

The objective is to integrate ERM at the business-domain level and incorporate ERM into normal, daily business process and cycles throughout the company's worldwide operations.

Annual Revenues (as of 9/29/2006) – US$1.8 Billion (Net)
Industry – Financial Services
Company Headquarters – United States
Number of Employees – 3,947

BUILDING AN ENTERPRISE RISK STRATEGY AT TD AMERITRADE

TD AMERITRADE's philosophy on ERM is allowing executive management to mitigate risk effectively while increasing the company's competitive advantage.

TD AMERITRADE is an online broker-dealer that has become a powerhouse in the financial services industry. With its acquisition of rival e-broker, TD Waterhouse USA, TD AMERITRADE took its place as the largest broker-dealer in the world, as measured by online equity retail trades. Today, TD AMERITRADE's 3,947 associates work in five primary locations: Jersey City, Baltimore, Fort Worth, Kansas City and Omaha, its headquarters. The company has $18.5 billion in total assets.

TD AMERITRADE is aligned around its clients, which cover three primary segments: the active trader, the investor and the registered investment advisor. The year 2001 was one of explosive growth for TD AMERITRADE, growth that was achieved at least partly through visionary leadership by TD AMERITRADE's executive team, which, at this crucial juncture, recognized the need to identify risk and capture opportunity as part of its successful evolution. The result: TD AMERITRADE's enterprise risk management (ERM) initiative.

Mike Head, managing director of corporate audit, and Jim Bollman, managing director and corporate risk officer, believe that the overall strength in TD AMERITRADE's ERM program is that co-ownership exists at the executive management level. This co-ownership includes collaboration between finance, audit, compliance and other business areas. The ERM program does not focus on one discipline, but rather, on the full scope of TD AMERITRADE's business components.

The company's ERM activities are based on the strategic business imperative of doing what is in the best interest of three groups:

- Shareholders
- Clients
- Associates

"This is our formal imperative," Head says. "If we do what is right and in the best interests of these people, we should be successful. Sometimes, this imperative is in harmony, and sometimes, it contrasts, but the key is to strike a balance and optimize results."

TD AMERITRADE adopted ERM in 2001, a time when many professionals were unaware of ERM as a strategy. "Mike had a vision to stretch risk management across all of our departments, organizations and business units, so that it would penetrate the company and establish a common risk language in everything we do," says Bollman.

Building ERM

According to Head, when he was hired, his first goal was to establish a COSO-based, risk-based internal audit function. The next step in that evolution was to extend the COSO framework to support an ERM program and risk assessment process across the business, with the support of executive management. "When you look at the ERM COSO-based framework, it aligns perfectly with where we are today," he says. The initial vision was to develop a framework that allowed management to assess and evaluate the internal control environment, along with a risk assessment process that encompassed the

entire company. Next, Head helped create the corporate risk office position and assisted in the hiring of Bollman to take on that role.

"Now we are at the stage where we must assess our risk and ensure that our control and monitoring activities are continually realigned toward the most significant risks facing the company, both internally and externally," Head says.

The overall structure of TD AMERITRADE's ERM program is a combination of the corporate risk committee, which is comprised of the company's executive management, and the Strategic Risk Assessment (SRA) workshop, which allows the executives to identify critical risk events and document them using the COSO framework. "Working alongside the corporate risk committee are approximately seven or eight subcommittees that are embedded in TD AMERITRADE's daily business operations," says Bollman. "These subcommittees manage, monitor and report to the corporate risk committee from an oversight point of view on the day-to-day management and mitigation of risk. We see the focal point of our ERM strategy as our corporate risk committee, which is sponsored by the audit committee."

Overall, the SRA workshops have two parts. One is the workshop, which takes a top-down approach to risk. The other is the committee structure, a bottom-up approach. "The corporate risk and corporate audit teams are in the middle, facilitating risk metrics, such as frequency, severity, probability and likelihood. We 'mind the gap,'" says Bollman.

Another unique aspect of ERM at TD AMERITRADE involves the resources dedicated to the program. "We have a staff of 2,100," Bollman says, referring to TD AMERITRADE's entire employee population. "Two thousand one hundred employees comprise our risk management team. They use a common language and common risk metrics."

Head adds, "There are two key parts of our ERM success. The first is that we did not recreate risk management for the company. We knew risk management was occurring daily, and our goal was never to centralize those efforts. As Jim says, we have more than 2,000 people managing risk every day on the front lines of the company. It was our role to identify where risk was being managed and how it was being monitored. We then identified the committees, groups and cross-functional teams that were managing silos of risk throughout the company and told them to continue what they were doing, but to operate under the oversight of the corporate risk committee.

"The second key of our success is that we established a disciplined approach to documenting, evaluating, communicating and evidencing risk mitigation at TD AMERITRADE," he says. "We measure our risk mitigation efforts, so that executive management and the corporate risk committee can ensure that we communicate and manage risks consistently across the company. We are the facilitators for helping TD AMERITRADE use a common risk framework and tools to manage risk in a way that is repeatable, systematic and routine, instead of haphazard."

Strategic tools

One way this was accomplished was through the use of the COSO matrices and Risk Navigator. The COSO matrices allow TD AMERITRADE associates to examine the "as is" state of risks across the organization. They also support an analysis of control gaps in facilitated sessions. The matrices are standardized and centralized repositories that give TD AMERITRADE an inventory of its risk universe.

"The matrices organize our risks, pulling them together along the strategic business objectives of the company and key ownership within the organization," Head says. "If you drilled down into our database, you would be able to see control matrices aligned according to our organizational structure that tie back to the key business strategies established by management. When we did this manually, it was an administrative hurdle. Now, it is automated through Risk Navigator."

Risk Navigator is a desktop interface that fits perfectly with the company's technology-based business culture. "The desktop highlights the risks associated with an associate's job, as well as the controls that correspond with those risks," Bollman says. "Our associates can add risks, control activities and

action plans as their jobs evolve, making this a dynamic tool. All of the changes roll up to supervisors, enabling us to manage these risks quickly and effectively."

TD AMERITRADE transitioned from manual processes to the Risk Navigator database in the summer of 2005. Head and Bollman have just completed the fiscal year 2006 SRA workshop and have identified dynamic shifts in the company's risk profile. They are now exploring those critical risk events through their strategic tools, and look forward to going through the first full cycle using the Risk Navigator in the coming year.

Benefits of TD AMERITRADE's ERM program

One clear benefit with TD AMERITRADE's approach to ERM is that it leverages each one of the company's associates. The Risk Navigator allows the identification and modification of risk awareness to be accomplished through several clicks on a computer screen. "There is a significant increase in risk awareness, ownership and accountability," says Head. "This tool has taken that to the next level for us – a huge benefit."

Other benefits include:

- Automation of the maintenance and inventory of risk
- Automation of a common risk language
- Implementation of a "point and click" company risk profile
- Establishment of risk prioritization and linkage among the audit committee, executive management and line management, with regard to risk ownership
- Incorporation of a clear risk strategy that is articulated and documented, and can be shared with external parties

While these are all important benefits, two more stand out as what Head calls "home runs." First, he says, "When examining our risk profile, as perceived by our underwriters, insurance agents, and those that provide what I consider critical transfer of risk coverage for directors and officers and errors and omissions, it becomes clear that in some cases we would not have been insurable without this process in place. In all cases, we get deeper and higher discounted premiums, so we are getting better risk management for lower costs. That is a significant benefit that we can track, measure and report."

Second, through automation, TD AMERITRADE has minimized the incremental costs necessary to facilitate, administer and coordinate its robust ERM process. "This is why we can achieve results with one dedicated risk management professional in the company," says Head. "We are leveraging existing resources and technology."

However, the automation itself was one of the biggest challenges TD AMERITRADE faced in establishing ERM. Another was identifying the touchpoints in the committee structure. "We had to identify all the individuals who would have an impact on a particular risk, and that was a challenge," he says.

Performance metrics

TD AMERITRADE tracks a number of metrics and uses a scorecard approach based on the declining total cost of risk to revenues percentage. "Corporate surveys tracking what organizations are spending on insurance premiums and uninsured claims help us benchmark against competitors," Bollman says. "We also add up all of our unexpected costs, such as those associated with arbitrations, litigations and discontinued operations, and we call that our total cost of risk. We divide that cost by our revenues each quarter to see how we are doing. We began this metric about two years ago, and it has been slowly declining, which is representative of how we are controlling risk on a hard-dollar basis," he says.

On a more qualitative basis, TD AMERITRADE measures the completion of its internal control assessment program and certification, not only on financial internal controls and reporting, but on all controls,

including operational efficiency, effective compliance with laws and regulations, and accuracy and completeness of financial statements. This is done quarterly and is a critical success factor for the company.

The true test of ERM

Head has this caveat for organizations implementing an ERM approach: "If someone thinks that a best practices ERM program will prevent losses or other issues from occurring, they are wrong. You can't be competitive if you are risk [averse]. However, ERM can help you better allocate resources and respond more quickly and effectively to risk."

"Our vision of ERM is that it should allow executive management to effectively mitigate risk, while increasing competitive advantage," he says. "The effective management of risk is not just avoiding hazards, although as we evolve, ERM will enable us to get better at identifying and preventing hazards on a timely basis. We want to use our ERM program as a competitive advantage. If we have our arms around our regulatory environment and what our customers need and want, and if we are managing the associated risks more effectively, we are going to be more competitive in the marketplace. ERM should be used as a tool for core competitive advantage as opposed to prevention."

Annual Revenues (as of 12/31/2006) – £3.1 Billion (Net)
Industry – Engineering/Manufacturing
Company Headquarters – United Kingdom
Number of Employees – 37,000

INTEGRATING ERM WITH STRATEGY AT TOMKINS PLC

Tomkins plc, a global engineering and manufacturing group, attributes the success of its ERM initiative to support from top management and a relevant practical approach.

Tomkins plc is a world-class global engineering group with market and technical leadership across two business segments: Industrial & Automotive and Building Products. The Industrial & Automotive group supplies industrial and automotive original and replacement equipment to markets around the world. The Building Products group is a leading manufacturer of building construction components in North America, providing supplies to residential and commercial construction markets, as well as manufactured home and recreational vehicle markets.

Tomkins began its enterprise risk management (ERM) effort in 2000 to meet the implementation deadline for the U.K.-issued corporate governance guidelines under the Combined Code. The Combined Code, stemming from similar drivers that shaped Sarbanes-Oxley in the United States, takes a more flexible "comply or explain" approach, and includes provisions whereby U.K. companies are to establish a system of internal controls that includes an ongoing process for identifying, evaluating and managing the significant risks faced by the company. Company directors are to issue an annual report to confirm both risk management processes and internal control frameworks support overall corporate governance standards. Tomkins' ERM became a cornerstone of its Performance Management Framework, an important factor in sustaining ERM over the long term.

To adhere to these mandates, Tomkins began by establishing an overall framework to facilitate the risk identification process, defining specific categories and subcategories for enterprisewide risk, such as strategic, operational, financial and compliance. Once the initial risk framework was defined, the company developed reporting templates for Risk Profiles, which are risk maps plotting risk likelihood and impact.

From 2002 to 2006, Shawn Tebben* served as the vice president of Tomkins' Risk & Assurance Services. In this role, she was supported by six staff members who divided their time between ERM and the company's internal audit function. Tebben reported functionally to the audit committee and administratively to the CFO.

"In 2001, once the risk framework and supporting templates were developed, my predecessor conducted a series of ERM workshops across the organization," she says. "Tomkins is a highly decentralized organization, with a number of subsidiaries that operate independently of one another."

"This means that different management teams were involved in each of the sessions. External facilitators and anonymous voting technology were used in the workshops, and the end results included Risk Action Plans that were linked to the Risk Profiles."

Both the Risk Profiles and the Risk Action Plans were meant to capture and help management focus on the risks that could be the most disruptive or costly to the company. They have evolved since then. "The overall goal at the time was for management to be able to demonstrate to the board of directors that we had a risk management process in place and that we were in compliance with the Combined

*Since this profile's original publication in 2006, Ms. Tebben has left Tomkins plc and now works for Protiviti as a managing director in Denver.

Code. No one had the illusion that this was a simple, one-time-only effort. We knew that it would be an ongoing evolution," says Tebben. "And it has been."

ERM and strategy

Tebben's predecessor was responsible for establishing and rolling out ERM-related methodology and tools across Tomkins. It was then up to the local and subsidiary management to maintain and sustain the Risk Profiles, with periodic validation by the vice president of Risk & Assurance Services. The management teams of the 15 or so largest subsidiary groups individually met on a periodic basis to discuss their Risk Profiles, reassess the context in which they were reporting risks and confirm the substance of the Risk Action Plans.

When Tebben joined to lead the team, it soon became clear that ongoing risk assessment should be more clearly linked to core business strategies. "During the third and fourth years of ERM implementation, we revisited our overall framework and updated our risk reporting tools," she says. "It was through that process that we also updated the approach used in the facilitated sessions, which are now internally led. The momentum is always very strong in the early days, but unless ERM is revisited and refined and, importantly, integrated into an ongoing management process, it can quickly become just another report to corporate. Our goal was and is to make sure that ERM is integrated with strategy, something we've focused on as we continue to reinvigorate and embed the ERM process. We coach our management teams on sustaining ERM going forward by establishing internal accountability."

As a result, Risk Profiles have become a recurring subject at monthly and quarterly management meetings. "The individuals in these meetings are talking about their Risk Profiles and identified improvement actions. ERM has become more integrated with strategy because everyone sees the need to discuss it on an ongoing basis – not just once a year. One way we achieve this awareness is by using strategic business objectives as a starting point in all of our facilitated risk assessment sessions, ensuring that our risk brainstorming is targeted and focused on business goals. This approach helps propel ERM as a tool for monitoring and achieving strategic objectives, and as a result, executive management sees ERM as adding real value to the organization."

Tebben and the risk and assurance team provided the board of directors with a Group Risk Profile and Group Risk Response Assessment, which depicted risks on both the business unit and corporate levels. Importantly, the group-level reports are validated by the executive management team, keeping ownership squarely with management.

Tebben also periodically reported to the audit committee on specific risk management activities. She participated in quarterly operational reviews involving executive management and business units, which enabled her to provide assurance to the audit committee of the organization's risk awareness and transparency.

The benefits and challenges of ERM

As a tool or methodology for supporting strategic objectives, ERM demonstrates clear value. To strengthen ERM as a tool, Tebben instituted a Risk Response Assessment rating to the process, allowing risks to be ranked by limited, moderate or substantial scope for improvement. Risks that are rated moderate or substantial should include committed improvement actions, which in turn are used by management for tracking and monitoring progress. "This is an example of ERM as a tool and a technique, rather than just a pretty picture," says Tebben. "The feedback I receive from management is that the improvement actions are where they see real value. Over time, they have become satisfied that ERM does not just stop with identifying the risks." Tebben points out that ERM also helps increase companywide knowledge of risk by incorporating risk awareness in the corporate culture.

The most significant challenge of ERM at Tomkins was embedding and sustaining the process. "It's hard to make ERM tangible and useful," Tebben says. "If you get overly creative and try to refine this down to a science, you may lose the benefit you're trying to create in that it may become an annual

reporting cycle and nothing more. Consistency in assessing the risk is a challenge, as well; you can provide guidance on assessing impact and likelihood, but some management teams will think of risk differently than others. Keeping the context consistent is difficult."

Two critical success factors that Tebben cites are executive management support for ERM and the part-time appointment of an ERM champion in each business unit. "ERM has to be relevant and practical for leadership in order for it to be successful," she says. "Having risk management champions who are already in the business, rather than having me periodically dip in and out of each business unit, is essential to this initiative as well. The risk champions have to be part of the business, facilitating the updates and helping management to keep the process alive."

Embedding ERM in core processes is easier when it is a standing agenda item in operational reviews and incorporated into various operational processes. For example, ERM is an explicit part of Tomkins' Investment Project Proposal (IPP), or capital allocations, process. "Since the IPP process involves risk assessment, capital allocation has a risk dimension to it," says Tebben. "Those in charge of an IPP have to assess the risks involved in the project, and if the risks are high impact, they are asked to articulate their Action Plans to manage those risks. A risk reference tool is embedded in the IPP forms, providing prompts or considerations that help the reviewers generate discussion around the identified risks." A similar risk reference tool, stemming from past due diligence reports, is used for mergers and acquisitions.

Lessons learned

In 2005, Tebben and her team reinvigorated the ERM process by reconnecting with the businesses. "It has been a cycle," she says. "There was a lot of initial momentum which, of course, dies down eventually. At that point, the risks that are reported often become tactical and operational rather than strategic in nature. When you go back and conduct facilitated sessions again, the Risk Profiles change quite a bit."

She adds, "It's important to recognize that ERM is not a one-time effort. You cannot establish the process and expect it to go on forever without real effort and executive support. You have to revisit, update and refine it periodically, and even then it will take a couple of cycles for it to be truly ingrained in the culture."

ABOUT PROTIVITI

Protiviti (**www.protiviti.com**) is a leading provider of independent risk consulting and internal audit services. We provide consulting and advisory services to help clients identify, assess, measure and manage financial, operational and technology-related risks encountered in their industries, and assist in the implementation of the processes and controls to enable their continued monitoring. We also offer a full spectrum of internal audit services to assist management and directors with their internal audit functions, including full outsourcing, co-sourcing, technology and tool implementation, and quality assessment and readiness reviews.

Protiviti, which has 60 locations in the Americas, Asia-Pacific and Europe, is a wholly owned subsidiary of Robert Half International (NYSE symbol: RHI). Founded in 1948, Robert Half International is a member of the S&P 500 index.

Among Protiviti's many publications are:

- *Making Sarbanes-Oxley Compliance More Cost-Effective While Improving Quality and Sustainability*
- *Internal Audit Capabilities and Needs Survey*
- *Internal Auditing Around the World, Volumes I, II and III*
- *Top Priorities for Internal Audit in a Changing Environment*
- *Guide to the Sarbanes-Oxley Act: Managing Application Risks and Controls, Frequently Asked Questions*
- *Guide to Enterprise Risk Management: Frequently Asked Questions*
- *Partnering with the Rest of the Board*
- *Protiviti Risk Barometer*
- *Guide to the Sarbanes-Oxley Act: Internal Control Reporting Requirements, Frequently Asked Questions Regarding Section 404*
- *Guide to Business Continuity Management: Frequently Asked Questions*

In addition, Protiviti publishes *The Bulletin*, a periodic newsletter covering key corporate governance and risk management topics of interest to internal auditors, board members and C-level executives.

For a copy of any of our publications, please visit **www.protiviti.com** or call **1.888.556.7420**.

KNOWLEDGELEADER[SM] PROVIDED BY PROTIVITI

KnowledgeLeader[SM] (**www.knowledgeleader.com**) is a subscription-based website that provides information, tools, templates and resources to help internal auditors, risk managers and compliance professionals save time, stay up-to-date and manage business risk more effectively. The content is focused on business risk, technology risk and internal audit, and is updated weekly.

The tools and resources available on KnowledgeLeader include:

- Audit Programs – A wide variety of sample internal audit and IT function audit work programs are available on KnowledgeLeader. These work programs, along with the other tools listed below, are all provided in downloadable versions so they can be repurposed for use in your organization.
- Checklists, Guides and Other Tools – More than 400 checklists, guides and other tools are available on KnowledgeLeader. They include questionnaires, best practices, templates, charters and more for managing risk, conducting internal audits and leading an internal audit department.
- Policies and Procedures – KnowledgeLeader provides more than 200 sample policies to help in reviewing, updating or creating company policies and procedures.
- Articles and Other Publications – Informative articles, survey reports, newsletters and booklets produced by Protiviti and other parties (including *Compliance Week* and Auerbach) about business and technology risks, internal audit and finance.
- Performer Profiles – Interviews with internal audit executives who share their tips, techniques and best practices for managing risk and running the internal audit function.

Key topics covered by KnowledgeLeader:

- Business Continuity Management
- Control Self-Assessment
- COSO
- Credit and Operational Risk
- Enterprise Risk Management
- Fraud and Ethics
- Internal Audit
- Sarbanes-Oxley and Corporate Governance
- Security Risk
- Technology Risk

Also available on KnowledgeLeader – Methodologies and Models, AuditNet Premium Content, discounted certification exam preparation material, discounted CPE courses, white papers, audit, accounting and technology standards, and best business links.

To learn more about KnowledgeLeader, sign up for a complimentary 30-day trial by visiting **www.knowledgeleader.com**. Protiviti clients and alumni, and members of The IIA, ISACA, the AICPA and AHIA, are eligible for a subscription discount. Additional discounts are provided to groups of five or more.

Introducing KLPlus℠ (KL+)

KnowledgeLeader members have the option of upgrading to KL+. KL+ provides all of the benefits of KnowledgeLeader, and for 50 percent or more off of the standard price, full access to Risk Solutions iTraining (see the following iTraining section).

PROTIVITI'S RISK SOLUTIONS iTRAINING DEVELOPMENT SERIES

Protiviti's Risk Solutions iTraining is a comprehensive collection of interactive, Internet-based training courses offering a rich source of knowledge on internal audit and business and technology risk management topics that are current and relevant to your business needs.

Topics include:

- Introduction to Self-Assessment
- Testing and Controls
- Information Technology (IT) Audit
- Enterprise Risk Management
- Audit Project Management
- Sarbanes-Oxley Act Compliance

Composed of materials originally developed for training Protiviti's consulting professionals, these courses are designed to give organizations and individuals a high-quality learning experience in a convenient format. The wide array of courses provides process owners, general management, boards of directors and other professionals with continuing education opportunities they can access anytime via the Internet. Protiviti's iTraining offerings also qualify for CPE credit.

This content can give you and your employees a significant advantage as you face continuing regulatory, corporate governance and internal control challenges. Courses incorporate real-life knowledge and practical skills that can be immediately applied within the work environment.

For more information, visit **www.protiviti.com**.

The Americas

UNITED STATES
+1.888.556.7420
protiviti.com

BRAZIL
+55.11.5503.2020
protiviti.com.br

CANADA
+1.416.350.2181
protiviti.ca

MEXICO
+52.55.5726.6612
protiviti.com.mx

Europe

FRANCE
+33.1.42.96.22.77
protiviti.fr

GERMANY
+49.69.963768.100
protiviti.de

ITALY
+39.02.655.06.301
protiviti.it

THE NETHERLANDS
+31.20.346.04.00
protiviti.nl

UNITED KINGDOM
+44.20.7930.8808
protiviti.co.uk

Asia-Pacific

AUSTRALIA
+61.3.9948.1200
protiviti.com.au

CHINA
Mainland
+86.21.3401.4630
protiviti.cn
Hong Kong
+852.2238.0499
protiviti.cn

INDIA
+91.11.4051.4198
protiviti.in

JAPAN
+81.3.5219.6600
protiviti.jp

SINGAPORE
+65.6220.6066
protiviti.com.sg

SOUTH KOREA
+82.2.3483.8200
protiviti.co.kr

Protiviti is a leading provider of independent risk consulting and internal audit services. We provide consulting and advisory services to help clients identify, assess, measure and manage financial, operational and technology-related risks encountered in their industries, and assist in the implementation of the processes and controls to enable their continued monitoring. We also offer a full spectrum of internal audit services to assist management and directors with their internal audit functions, including full outsourcing, co-sourcing, technology and tool implementation, and quality assessment and readiness reviews.

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

protiviti.com