CBIZ MHM Special Report

THE EMERGING FRONTIERS OF RISK MANAGEMENT

The Emerging Frontiers of Risk Management

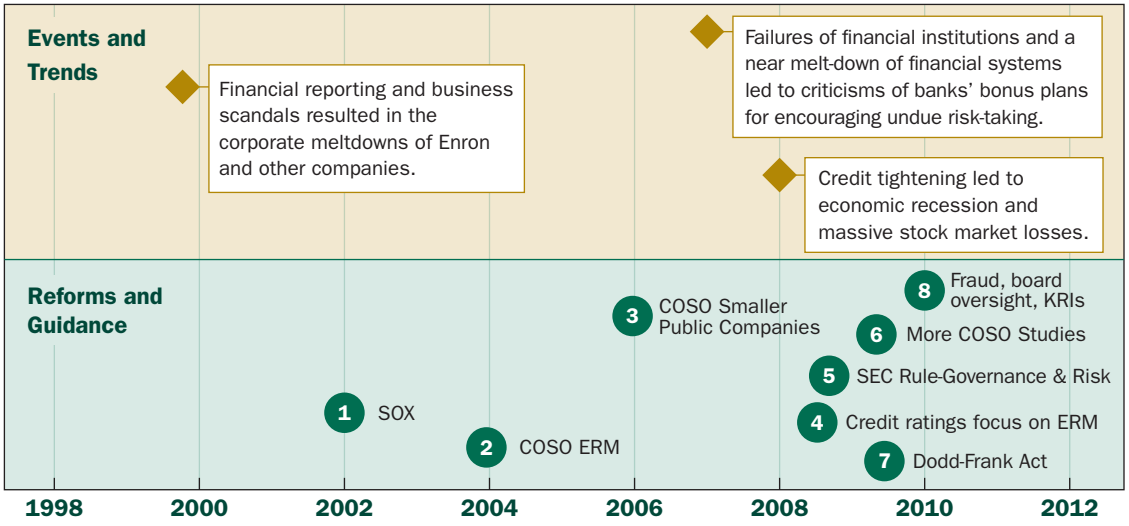
TODAY'S NORMS AND EXPECTATIONS

Ten years ago, businesses and investors entered a decade of wrenching change. Enterprise risk management (ERM) was a relatively undeveloped field then, and few businesses had the policies and practices needed to protect their stakeholders from the effects of the severe financial and economic crises of 2008 and 2009. Since then, the overall state of readiness has improved. But new challenges continue to emerge every day, and surprises are still possible. How well prepared is your company for the risks, expectations, and stresses on internal controls that lie ahead? This report will help you understand how your company compares with others and what steps you can take now to improve the way you manage risks.

A Decade of Mounting Expectations

The norms and expectations for risk management have evolved over the past decade as a result of changing economic and business conditions that were well-publicized by the media. Some of the media reports fueled a sense of public outrage over significant losses due to unexpected risks. With each wave of outrage came more calls for "no surprises" followed by rounds of guidance, regulatory reforms, and enforcement actions. The reforms and guidance peaked toward the end of the decade, helping companies to find better ways to meet the mounting expectations of investors, customers, credit rating agencies, regulators, and others — all of whom are demanding higher standards of governance, risk management and compliance.

Milestones on the Road to Better Risk Management



Milestones on the Road to Better Risk Management *(continued)*
Key to reforms and guidance

1. Congress enacted the Sarbanes-Oxley Act of 2002 (SOX), introducing new Internal control reporting requirements.

2. COSO published "Enterprise Risk Management-Integrated Framework"- an expansion of the COSO Internal Control-Integrated Framework published in the 1990s.

3. COSO published "Internal Control over Financial Reporting - Guidance for Smaller Public Companies."

4. Major credit rating agencies Standard & Poor's and Moody's intensified their reviews of risk management programs employed by both financial and nonfinancial companies. S&P published progress reports on integrating ERM Analysis into ratings.

5. New SEC rules took effect for the 2010 proxy season, resulting in required disclosures about the role of the board of directors in risk oversight, as well as any compensation policies and practices that present material risks to the company.

6. COSO published the results of a study on "Fraudulent Financial Reporting: 1998-2007."

7. Congress enacted the Dodd-Frank Wall Street Reform and Consumer Protection Act. Among other things, this Act exempts smaller public companies from the SOX requirements for auditor attestation of internal control reporting.

8. COSO released additional reports, including:
   - 2010 Report on ERM: Current State of Enterprise Risk Oversight and Market Perceptions of COSO's ERM Framework.
   - Board Risk Oversight: A Progress Report.
   - Developing Key Risk Indicators to Strengthen ERM.

Evolving Yardsticks Of Success

Although there are several risk management frameworks available today, the COSO guidance has become key to measuring success. COSO stands for the Committee of Sponsoring Organizations of the Treadway Commission. This Committee is a voluntary private-sector organization committed to publishing studies and thought papers that expand the bodies of knowledge in the areas of internal control, enterprise risk management and fraud deterrence. COSO's guidance on risk management has helped to light the way forward, but progress has been uneven and difficult to measure – in part because of the need for judgment in assessing the extent to which an entity is meeting the multi-dimensional parameters necessary for a formal ERM program as defined by COSO.

Definition of ERM

A process, effected by an entity's board of directors, management, and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.

COSO, Enterprise Risk Management Framework, 2004

Because considerable judgment is required to gauge the level of progress on some of the parameters, (e.g., managing risks within risk appetites and providing reasonable assurance of objectives across an enterprise), there is no convenient way to rate a company's overall risk management performance against others of its size or in its industry. But some qualitative data is available about specific benchmarks on the journey to ERM. Comparisons with these benchmarks can be helpful in communicating with boards and investors who want to know where a company stands and how well it is meeting the expectations of investors, customers, credit rating agencies, regulators, and others.

Questions to Ask to Determine Where You Stand

Within the context of the COSO definition cited above, the following questions illustrate the kinds of benchmarks that may be helpful in determining where a company stands relative to overall norms and expectations:

1. Does the company maintain a "risk register" or "heat map" that classifies top risks by likelihood and impact, along with a mitigation strategy for each?
2. Does the company assign specific ownership for key risks?
3. Does the company develop alternative mitigation strategies?
4. Does the company communicate risk tolerances across the organization?
5. Does the company clearly communicate risk appetite to internal and external stakeholders using a standard and consistent ERM language?
6. Does the company have a fully engaged and risk-astute board of directors overseeing risk?

Answers: A "yes" answer to question 1 is the norm, (i.e., most common approach among companies that have a formal ERM program according to a 2010 report by S&Ps.) If you can answer "yes" to questions 2 through 4, then according to S&P's report, your company is one of a relatively small minority of high achievers. A "yes" answer to questions 5 and 6 means your company falls within an even more elite minority, despite the fact that stakeholders want and expect more information now about risk management. A major obstacle to providing this information seems to be the lack of a uniform language for risk that is understandable by everyone involved – line managers, senior executives, board members, shareholders, regulators, and other stakeholders.

For More Information

The COSO guidance mentioned in this report is available for purchase or download at **http://www.coso.org**. These materials include:

- COSO, Enterprise Risk Management — Integrated Framework, 2004.
- COSO, Internal Control over Financial Reporting — Guidance for Smaller Public Companies, 2006.
- COSO, Fraudulent Financial Reporting: 1998-2007 — An Analysis of U.S. Public Companies, 2010.
- COSO, Effective Enterprise Risk Oversight: The Role of the Board of Directors, 2009.

- COSO, Embracing Enterprise Risk Management: Practical Approaches for Getting Started, 2011.
- COSO, Developing Key Risk Indicators to Strengthen Enterprise Risk Management, 2010.
- COSO's 2010 Report on ERM: Current State of Enterprise Risk Oversight and Market Perceptions of COSO's ERM Framework, 2010.

Other materials mentioned in this report are available for download from the following sources:

- Standard & Poor's, Credit FAQ: Standard & Poor's Looks Further into How Nonfinancial Companies Manage Risk, June 24, 2010. (**http://www.standardandpoors.com/ratings/erm/en/us**)
- US Securities and Exchange Commission, Final Rule on Proxy Disclosure Enhancements, December 2009. (**http://www.sec.gov/rules/final/2009/33-9089.pdf**)
- Sarbanes-Oxley Act of 2002. (**http://fl1.findlaw.com/news.findlaw.com/cnn/docs/gwbush/sarbanesoxley072302.pdf**)
- Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010. (**http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111_cong_bills&docid=f:h4173enr.txt.pdf**)

The Emerging Frontiers of Risk Management

FRAUD AND RELATED RISKS

The risk environment is constantly changing, challenging companies to monitor the changes and focus their efforts on the most pressing issues at any point in time. In recent years, fraud has been an area of growing concern for companies of all sizes. A 2010 report by the Institute of Internal Auditors (IIA) indicates that frauds have been more prevalent since the onset of the economic recession in 2008, especially employee-related frauds such as theft of company property and resources, embezzlement, and expense account fraud. The IIA's report explains that these types of frauds have increased as the economic recession and accompanying unemployment levels have affected countless employees on a personal level, often involving the loss of income from one or more household members.

Making Fraud a Higher Priority

The rising level of fraud has prompted many companies to develop and implement proactive anti-fraud programs designed to detect and prevent all kinds of fraud, including employee-related frauds. In one well-publicized fraud case, a report in Compliance Week estimated that the amount misappropriated over a five-year period nearly equaled the company's market capitalization. Reports like this one are causing other companies to ask, "Could it happen here?"

Could fraud be occurring at your company?

Recently it was revealed that over $30 million was stolen from Milwaukee-based Koss Corporation (the Company), allegedly by senior members of the accounting team. According to the FBI's indictment, this fraud was perpetrated by the authorization of numerous wire transfers of funds from bank accounts maintained by Koss to settle personal American Express credit card bills. In addition, the perpetrators used money from Koss's bank accounts to fund other personal expenses.

The fraudulent transactions were concealed from the Company by preparing false accounting books and records. This included false journal entries to disguise the misappropriation of funds. The perpetrators attempted to hide the embezzlement in the Company's financial statements by overstating assets, expenses, and cost of sales, and by understating liabilities and sales.

Based on the fraudulent accounting books and records the Company prepared materially false financial statements and filed materially false current, quarterly, and annual reports with the Securities & Exchange Commission. After discovering the embezzlement, the Company amended and restated its financial statements for fiscal years 2008 and 2009 and the first quarter of fiscal year 2010 (through September, 2009).

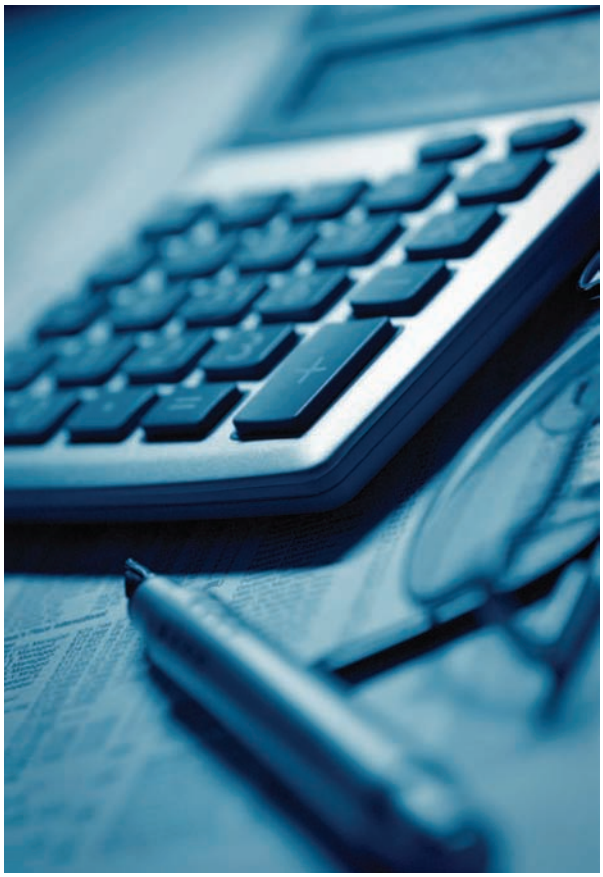
ADAPTED FROM: DEPARTMENT OF JUSTICE PRESS RELEASE, JAN. 20, 2010 AND SEC AAER NO. 3180 AND 3230, SEPT. 1, 2010 AND JAN. 13, 2011

Newly-Emerging Frauds and ERM

The assignment of higher priorities to programs that detect and prevent employee frauds is consistent with the integrated framework for Enterprise Risk Management (ERM) developed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), and it underscores the importance of managing risks related to business objectives. COSO's framework has four categories of objectives (strategic, operational, reporting and compliance). Employee frauds can affect all four categories because the full impact of these frauds typically extends beyond the amount misappropriated. For example, employee frauds can take a heavy toll on the company's reputation, as well as its relationships with shareholders, creditors, suppliers, customers, and others. These pervasive impacts are expected to continue as emerging trends will likely trigger additional forms of frauds that will have similarly far-reaching consequences.

A recent IIA study identified the following emerging trends and related risks:

- Additional forms of employee-related risks are emerging in difficult economic times. Examples include risks associated with lower compensation levels, (i.e., reduced or frozen salaries or bonuses), and risks associated with new employees or other employees who do not fully understand their job duties.



- Companies may also face more risks of frauds related to vendors or other third parties. Examples include overpayments to contractors and payments for services not rendered.
- Corruption-type risks related to compliance with laws may also increase. Examples include bribery of foreign officials, illegal side agreements, and facilitation payments related to imports.
- New forms of data and information risks are also emerging. Examples include disclosure of corporate data to competitors, use of information technology to cover up fraud, and risks associated with new financial systems.

Measures of Effectiveness and Assurance

Companies need reliable measures of progress to manage the full spectrum of frauds and related risks. COSO's broadest yardstick of success is helpful because it defines effectiveness broadly in terms of managing risks related to all four key categories of objectives: strategic, operational, reporting, and compliance.

Effectiveness

When enterprise risk management is determined to be effective in each of the four categories of objectives, respectively, the board of directors and management have reasonable assurance that they understand the extent to which the entity's strategic and operations objectives are being achieved, and that the entity's reporting is reliable and applicable laws and regulations are being complied with.

COSO, Enterprise Risk Management Framework, 2004

This definition of effectiveness requires a level of assurance that goes beyond that provided by external audits. External audits focus on exposures that can result in a material misstatement of financial statements or a material loss to the organization. They are not designed to assess whether the exposures are consistent with a company's risk appetite and achievement of its goals, but there is some synergy between financial statement audits and risk management because many fraud risks can be addressed with an appropriate system of internal control. The Sarbanes-Oxley Act of 2002 (SOX) paved the way for significant progress in that regard by requiring management reporting and auditor attestation on internal controls over financial reporting for public companies.

However, the Dodd-Frank Act of 2010 exempted smaller public companies (non-accelerated filers) from the auditor attestation requirements.

Growing Challenges for Smaller Companies

The SOX exemption for smaller public companies is both a blessing and curse. On the one hand, smaller companies are less able to foot the bill for costly auditor attestations; on the other hand, studies show they are more vulnerable to fraud. This creates an unlevel playing field for investors.

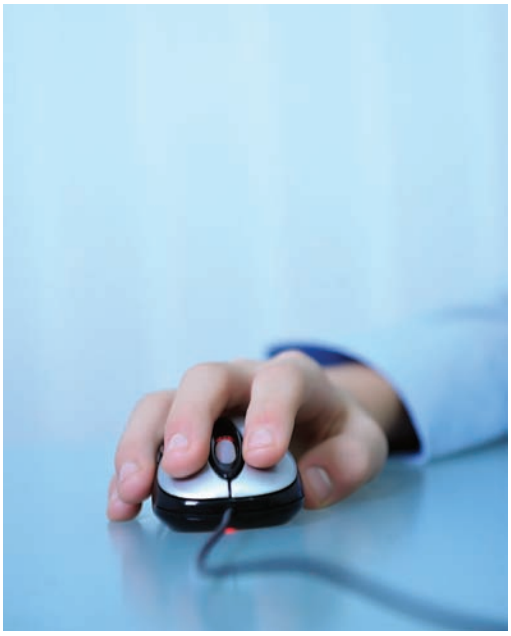
> **An Uneven Playing Field**
> *Small organizations are disproportionately victimized by occupational fraud. These organizations are typically lacking in anti-fraud controls compared to their larger counterparts which makes them particularly vulnerable to fraud.*
> **ACFE, "2010 Report to the Nations on Occupational Fraud and Abuse"**

Although the SEC is still studying the costs and benefits of the SOX requirements for smaller public companies, the status quo is particularly troublesome when it comes to fraud. A 2008 report by the Institute of Internal Auditors and others indicates that more companies are responding to expectations by expressing their risk appetite as a "zero tolerance" for fraud of any type. This objective is nearly impossible to achieve without supplemental programs for preventing and detecting fraud, especially in a smaller public company, where employees tend to be generalists who perform multiple job duties and it is more difficult to mitigate risks through segregation of duties or centralization of shared services.

Questions to Ask About Your Anti-Fraud Program

The following questions may be helpful in determining how well a company is managing its risk of fraud:

1. Has the company developed a statement of its tolerance for fraud? Is it approved by the board of directors?
2. Do the company's risk assessments take into account known frauds that have happened in companies of the same size and in the same industry?



3. Does the company have a strong and independent internal audit department? Is the internal audit function responsible for detecting and preventing fraud?
4. Does the company have effective fraud hotlines and whisteblower programs?
5. Does the company have a policy and methodology to investigate potential and actual occurrences of fraud?
6. Does the company build in effective internal controls, such as segregation of duties, to the extent practicable? Does it take other measures to mitigate the risk of fraud?
7. Does the company require mandatory vacation periods or job rotation assignments for employees in key positions in accounting and finance?
8. Does the company use a rigorous system of data analysis and continuous monitoring or auditing of items such as wire transfers and journal entries to detect fraudulent activity?

If the answers to any of these questions are "no," CBIZ can provide advisory services to help companies of any size in any industry to develop more proactive anti-fraud controls.

For More Information

The following materials are referenced in this report:

- COSO, Enterprise Risk Management — Integrated Framework, 2004
- Institute of Internal Auditors and Audit Executive Center, "Knowledge Alert: Emerging Trends in Fraud Risks," January 2010
- Melissa Klein Aquilar, "Small Filers Struggle with Internal Controls Over Fraud," Compliance Week, May 2010
- Institute of Internal Auditors (IIA), American Institute of CPAs (AICPA), and Association of Certified Fraud Examiners (ACFE), "Managing the Business Risk of Fraud: A Practical Guide," 2008
- Association of Certified Fraud Examiners (ACFE), "2010 Report to the Nations on Occupational Fraud and Abuse"

The Emerging Frontiers of Risk Management

REPUTATIONS, RELATIONSHIPS, AND OTHER STRATEGIC RISKS

Most business owners and managers recognize that a company's reputation and relationships with customers and suppliers rank high on the list of its most valuable assets. To preserve the value of these assets, business-savvy managers know they must go beyond traditional techniques for managing risks associated with physical and financial assets. The key is to find ways to protect and enhance corporate reputations and other intangibles that may never appear in a company's financial statements. This expanded focus helps companies maximize value, and it is becoming increasingly critical for maintaining and improving credit ratings. But it is not easy. The challenges include adapting to the stronger linkage between risk management and credit ratings, identifying strategic risks, and evaluating the potential consequences.

The Linkage Between Risks and Ratings

As part of the rating process, Standard & Poor's, Moody's and other rating agencies attempt to identify and assess each company's underlying value drivers, including the strength of its management and governance processes. The credit and financial crises of the late-2000s added impetus and urgency to these efforts because these events fueled public skepticism about the ratings assigned to a number of high profile corporate defaults that were attributed to weak risk management. Reactions to the credit crisis included criticisms of banks' bonus plans for encouraging undue risk-taking. Soon, the concerns spread to encompass the risk management techniques of companies in other industries as well.

In 2008, Standard & Poor's (S&P) announced its plans to widen the scope of its analysis of some nonfinancial companies by applying enterprise risk analysis to its corporate ratings of these companies. As part of this effort, S&P initiated discussions with management on the following topics:

- Management's view of the most consequential risks faced by their firms, including the likelihood of the risks and the potential effect on credit.
- The frequency with which the top risks were updated and the nature of the updates.
- The influence of risk sensitivity on liability management and financing decisions.
- The role of risk management in strategic decision-making.

All these matters reflect a desire to know more about the role that risk considerations play when making strategic decisions. S&P's announcements and articles on the subject indicate that the rating agency views risk management as a key component of a company's culture. Broadly defined, culture includes matters such as communications, structures, incentives, and risk appetite. The agency inquires about these matters to obtain a better assessment of management's ability to identify, monitor and manage key risks that are endemic to the company's industry and that managers elect to take when running their businesses.

To adapt to the stronger linkage between risks and ratings and to demonstrate the soundness of their corporate cultures, companies need to establish robust risk management processes that can effectively identify, evaluate, and communicate their most consequential strategic risks.

Identifying Strategic Risks

The process of identifying the most consequential strategic risks is inherently difficult, and today's volatile business environment adds to the complexities involved. To begin the process, management often starts with a risk inventory or risk register, followed by an analysis of (a) the relative likelihood each risk will materialize and (b) the magnitude of the potential impact, if the risk does materialize, either individually or together with other risks.

Typically, a company's risk factors include both external and internal factors.

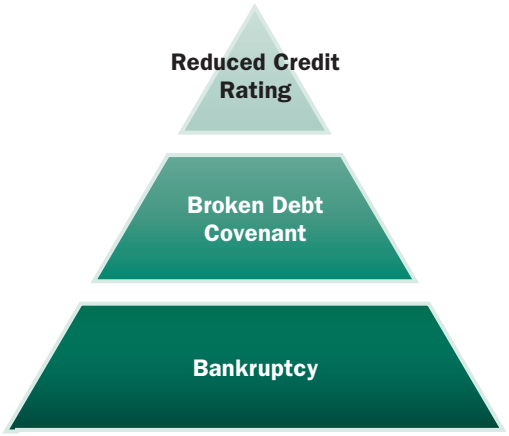
- **External factors** include changes in the industry, economy, competitors, customers, and legal or regulatory environment, including climatic risks and risks of terrorism or civil unrest.

- **Internal factors** include risks associated with the governance process used to oversee risks, the long-range planning process, or the bonus plans and other incentives used to reward risk-taking.

Evaluating the Consequences of Strategic Risks

The evaluation and governance of strategic risks typically involves a comparison with the company's risk appetite. In publicly-owned companies, the board of directors generally has some responsibility for helping ensure that a company's culture is aligned with its strategic plan and the risks taken do not exceed the company's risk appetite. In private companies and not-for-profit organizations, the responsibility typically resides with the managers or business owners. These individuals need appropriate information about the potential severity of the consequences of risks. This information can be aligned with three thresholds, comprising risks that might result in reduced credit ratings, broken debt covenants, and even bankruptcy.

The risk thresholds can be organized in a hierarchy as illustrated below.



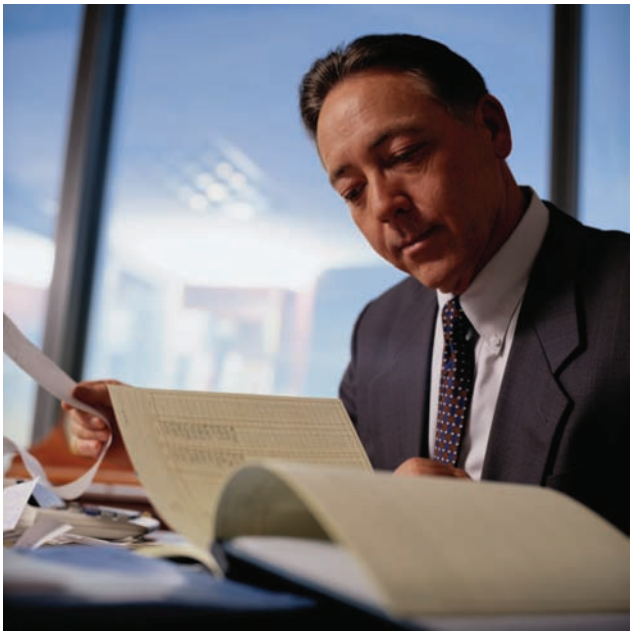
Although the precise consequences of each risk may be difficult to predict, management will likely be able to make a best-efforts estimate of the risks that cross these thresholds. Examples include events and trends that might limit a company's ability to adapt to changes in the economy, (such as volatility and spikes in prices of commodities), as well as those that affect its ability to fund and manage future growth, (such as regulatory changes affecting the launches of new products, entry into new markets, or negotiations of mergers and acquisitions). In companies with international customers or suppliers, strategic risks might also include potential

disruptions in supply chains or distribution channels due to catastrophic events, such as earthquakes or tsunamis. In smaller companies, the risks might include a lack of succession planning for top management.

Questions to Ask About Your Enterprise Risk Management Program

Enterprise risk management (ERM) is an evolving body of knowledge that helps companies to address a broad range of risks, including strategic risks. To ensure effective enterprise risk management and to prepare for discussions with external parties, such as regulators, creditors, and rating agencies, companies may find the following self-assessment questions helpful:

1. Is your company prepared to respond to inquiries from credit rating agencies about its risk culture, risk appetite, and risk management processes?
2. Has management made a systematic and thorough search for risks that might trigger reductions in credit ratings, broken debt covenants and even bankruptcy?
3. Does your risk management program consider risks related to economic conditions (such as price movements or capital availability) that might affect the cost of capital and thereby result in increased competition?
4. Does your risk management program consider risks related to the natural environment (such as floods, fire, or earthquakes) that might result in damage to plant or buildings, restricted access to raw materials, or loss of human capital?
5. Does your risk management program consider risks related to political factors (such as election of government officials with new political agendas or new laws and regulations) that might affect access to foreign markets or result in higher or lower taxes?
6. Does your risk management program take into account risks related to the social environment (such as changing demographics, work/life priorities, or terrorism activity) that might result in changing demand for products and services, new buying venues, human resource issues, or production stoppages?



7. Does your risk management program take into account risks related to technological factors (such as new means of electronic commerce) that might result in changes in the availability of data, infrastructure costs, or increased demand for technology-based services?

For More Information

The following materials are referenced in this report:

- Standard & Poor's, Ratings Direct, "Enterprise Risk Management: Standard & Poor's To Apply Enterprise Risk Analysis to Corporate Ratings"
- Standard & Poor's, May 7, 2008 and Credit FAQ: Standard & Poor's Looks Further into How Nonfinancial Companies Manage Risk, June 24, 2010

The Emerging Frontiers of Risk Management

INFORMATION TECHNOLOGY AND GROWTH

One of the most daunting challenges in today's business environment is to protect valuable data from a host of threats including vendor, security, and privacy risks. This area of enterprise risk management (ERM) is especially difficult given the pace of change in technology today. Each new day seems to bring new business models and new ways for customers to consume goods and services. IT professionals must stay on the leading edge of change to protect proprietary data and preserve the privacy of the company's customer base as a foundation for future growth. Effective oversight by business owners and boards of directors is equally important and every bit as critical. But both the necessary skills and the oversight have grown increasingly complicated and time-consuming in recent years, creating new challenges for both IT professionals and boards.

New Technologies and Broader Impacts

The introduction of "cloud" computing and wireless devices for ever more mobile workforces has increased the potential for sensitive information to migrate from laptops, to an even riskier base of i-phones, applications, and social media networks. Additionally, at the same time that technology is changing, a number of other factors are intensifying the risks related to the usage of the technology, both within and outside the company. Examples:

- The movements toward shared services, along with the growing acceptance of cloud computing and outsourcing of IT departments have introduced new risks. These forms of centralization often add cost efficiencies at the expense of traditional controls (such as onsite inspections of segregation of duties by management or internal auditors).
- Malicious damages have escalated from amateurish hacking pranks to threats of more sophisticated forms of cyberterrorism involving politically-motivated acts of deliberate, large-scale disruption of computer networks to further ideological agendas.
- A series of unprecedented events, ranging from hurricanes, earthquakes, and other natural disasters to massive oil spills and the bursting of the housing bubble – all underscore the importance of disaster recovery plans and backup facilities.

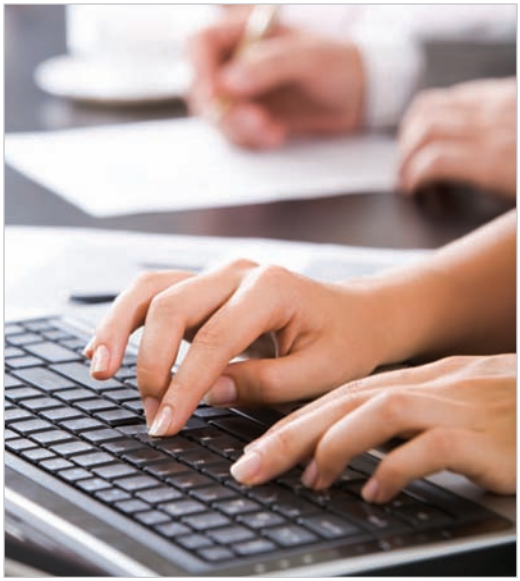
- The need for specialized technical knowledge has complicated management's ability to recruit, retain and promote its information technology workforce.
- Trends such as social networking and changing laws and regulations governing matters, such as internet usage and privacy rights, may require controls that are difficult to enforce as the responsibility for information security is shifting away from small handfuls of IT experts and into the hands of a wide group of individual users who may not share the same awareness of the need for security.

All these trends, individually and combined, are adding to the complexities and challenges of IT governance.
Two of the most difficult challenges involve identifying the assets at risk and establishing effective policies and responsibilities for oversight of IT risks.

Identifying the Assets at Risk

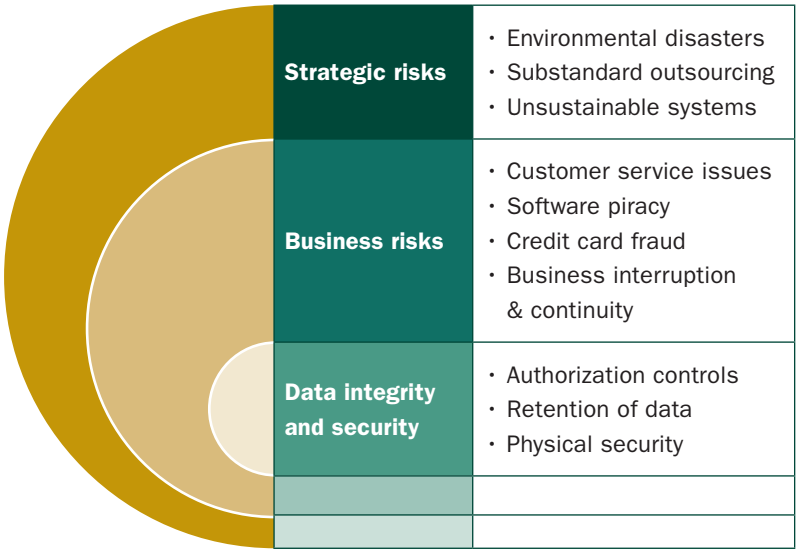
To cut through the complexities and ensure that their companies are focusing on the right risks at the right time, managers and directors are using ERM techniques that center around the concept of assets at risk. The underlying assets typically include proprietary data and other hard-to-value intangibles that may not appear on corporate balance sheets. The linkage is demonstrated in a series of questions that were summarized in a 2005 report by the Institute of Internal Auditors and include the following:

- **Risk identification**
  - What are the assets at risk and the value of their confidentiality, integrity, and availability?
  - What could happen to affect that information asset value adversely?
  - If a threat ever happened, how bad could its impact be?
  - How often might the event be expected to occur?
  - How certain are the answers to the first four questions?
- **Risk mitigation**
  - What can be done to reduce the risk?
  - How much will it cost?
  - Is it cost efficient?



Oversight of IT Risks

Because different areas of information technology can put the same assets at risk, the responsibilities for oversight of IT risks can present organizational challenges that compound the inherent complexities. More than ever before, effective oversight requires good coordination of input from technical experts, management, directors, and others. In effect, the layers of oversight are like concentric circles for different types of risks.



In publicly-owned companies, the board of directors will typically oversee the strategic threats that can put the entire company at risk, (e.g., an environmental disaster that might destroy essential systems and data). The board may also oversee the threats that put a business unit's customer base and other assets at risk, (e.g., serious customer service issues involving technology). And, depending on the value of the assets at risk, boards may also oversee data integrity and security risks, (e.g., when a lack of authorization controls is so serious as to compromise the integrity of a company's financial reporting system). To keep boards focused on the big picture issues, external auditors and risk advisors may be called upon to provide certain types of assurance and facilitate communications on the technical issues involved. In privately-owned and smaller companies, the responsibility for oversight of IT governance typically resides with the business owners and management teams.

For More Information

The following materials are referenced in this report:

- Institute of Internal Auditors, Global Technology Audit Guide, "Information Technology Controls," 2005

Questions to Ask About IT Risk Management

You may find the following questions helpful in determining how well your IT risk management processes stack up with other companies and what additional steps are needed:

1. Are board members or business owners adequately informed of the assets at risk?
2. Are valuations of off-balance sheet intangible assets sufficiently accurate and cost-effective?
3. Are management and boards appropriately informed of IT control weaknesses and failures?
4. Do all employees and contractors understand their responsibilities for data security?
5. Are data security controls evaluated for effects on end-users, including customers and business partners?
6. Does the company have an appropriate disaster recovery plan and business continuity plan?
7. Are plans and policies reviewed periodically to ensure applicability to new technologies?
8. Are recruitment, retention and development plans effective in ensuring up-to-date technical skills?
9. Are you sure your company has taken adequate steps to ensure its compliance with all the laws and regulations that apply to information technology?
10. Does management monitor proposed laws and regulations to ensure your company is fully prepared to comply with them?

If the answers to any of these questions are "no," CBIZ can provide assurance and consulting services to help you improve your company's IT risk management.

The Emerging Frontiers of Risk Management

COMPLIANCE AND FINANCIAL REPORTING

Throughout the 2000s, legislators and regulators unleashed a tidal wave of new laws and regulations and stepped up enforcement actions to better protect investors, customers, and employees from unexpected jolts due to risks that were not foreseen or mitigated. At the same time, accounting standard-setters stepped up efforts to converge US generally accepted accounting principles (US GAAP) with International Financial Reporting Standards (IFRS). The combination of these efforts left US-based companies dealing with significant uncertainties in compliance and reporting at the same time they were dealing with unprecedented uncertainties in the economy. Together, these factors both helped and hindered the journey toward better enterprise risk management (ERM). Many companies recognized the need for better risk management but had limited resources to adopt and implement robust ERM systems.

Changing Laws and Accounting Standards

Some of the most significant changes in laws, rules, regulations and accounting changes affecting companies today include the following:

- Major legislation was enacted in the US in response to financial reporting and credit crises, including the Sarbanes-Oxley Act of 2002 and the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010. The Sarbanes-Oxley Act introduced internal control reporting and auditor attestation requirements for all public companies, but smaller companies were later exempted from the attestation requirements. The Dodd-Frank Act introduced sweeping reforms for the financial sector as well as governance reforms that affect all sectors. The changes include a significant expansion of the SEC's powers to compensate whistle-blowers and greater shareholder rights, including votes on executive compensation.
- Recent US accounting standards and SEC rules have established additional requirements for disclosures about risks, and the US Financial Accounting Standards Board (FASB) is considering sweeping changes in accounting and financial reporting. The FASB has released a number of exposure drafts designed to converge US GAAP with IFRS. These proposals would make significant changes to US GAAP. Uncertainties remain regarding the final

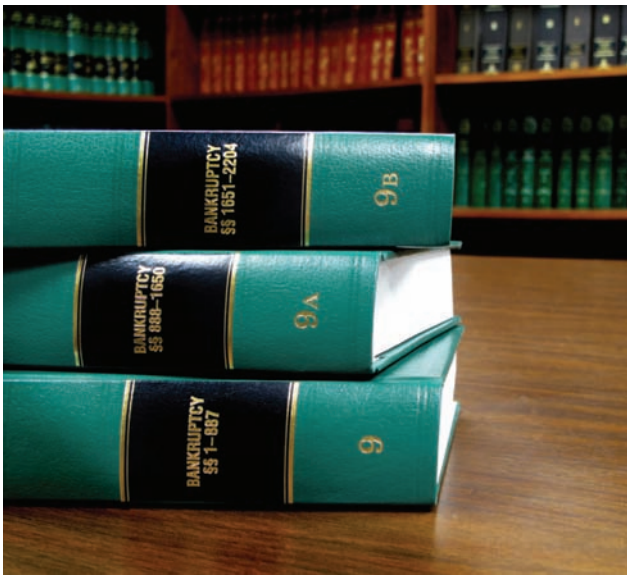
standards and effective dates, as well as when the SEC might require or permit US issuers to use IFRS in their SEC filings. The FASB is also considering a proposal for a separate US private company accounting standards-setting board.

- Some accounting changes initiated in the mid- to late- 2000s have had a delayed impact. For example, the FASB made significant changes to the accounting for business combinations under US GAAP in the late 2000s, but companies had relatively few occasions to implement these changes until the pace of activity in mergers and acquisitions (M&A) picked up in 2011.
- Many of the new laws and rules have significant tax implications. Most notably, changes in US tax laws have placed added emphasis on the reporting of uncertain tax positions for both accounting and tax purposes (IRS Schedule UTP), and the US is considering major tax reform for businesses for the first time in decades in an effort to lower the statutory rate and reduce budget deficits.

More "Grey Areas" and the Need for Greater Judgment

As a result of the increased volume of new laws and accounting standards, companies must devote more resources to monitoring and understanding the changing requirements. At times, the implications can be difficult to discern, and companies can find themselves in uncharted territories or "grey areas" that require considerable judgment and add to the risks related to compliance and financial reporting. Here are a few examples:

- **IFRS.** Changes in US accounting standards to achieve convergence with IFRS can have broad business implications that extend far beyond the accounting department, and a lack of interpretive guidance may have unintended consequences, such as a lack of comparability among financial statements or miscommunications with investors accustomed to US GAAP.
- **Taxes.** Schedule UTP, which is effective in 2011, introduces added tax risks because uncertain tax positions may need to be reported to the IRS before they are resolved. At the same time, companies may



face other new tax risks as the Obama Administration is considering a massive tax overhaul that may introduce yet more risks and uncertainties during the legislative and rule-making process.

- **M&A.** Accounting changes effective in 2009 make it more difficult for management to predict the earnings impact from potential acquisitions, and this increases the risks that may accompany M&A without increased due diligence and expert guidance in such areas as valuations and acquisition accounting.
- **Fraudulent financial reporting.** The SEC's expanded powers to compensate whistle-blowers could affect corporate hotlines in public companies. Currently, these hotlines are viewed as an important way to detect fraud. Some have expressed concerns about a risk that employees will report fraud to the SEC without reporting it to the company first.
- **Data security.** The Federal Trade Commission plans to start enforcing the Red Flags Rule in 2011. With limited exceptions, (e.g., for law and accounting firms), this rule applies to all companies that offer goods or services and allow customers to pay later. Under the rule, companies must take steps to detect identity theft, including written programs for accounts that present a "reasonably foreseeable risk from identity theft." This standard raises issues involving subjective interpretation.
- **Social networks.** US laws and enforcement actions about social networks raise legal questions not yet addressed by the courts, with the result that companies may need to walk a fine line between compliance and protecting their reputations. For example, enforcement actions by the National Labor Review Board indicate company policies for workplace use of social networking and related disciplinary actions for violations of the policy may be viewed as violating federal labor laws.

Oversight Challenges

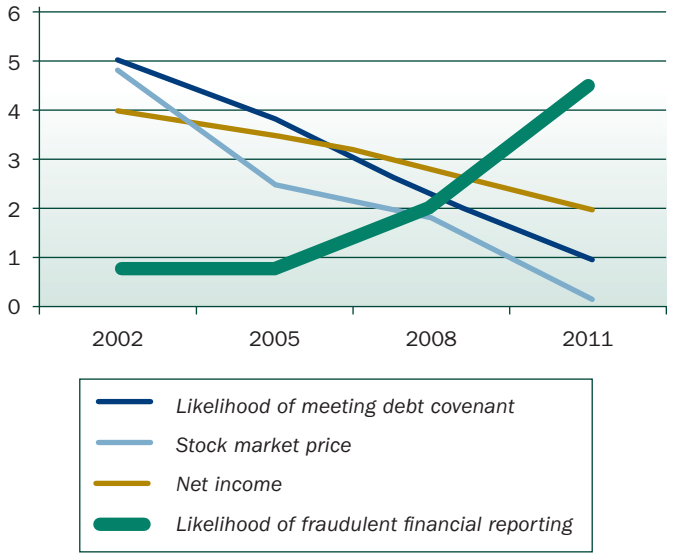
The challenges of overseeing compliance with standards, rules, and regulations are compounded by turbulent economic times. Studies show that the risks of fraud mount when there

are pressures to grow the business or when cost-cutting compromises internal controls. For example, a recent COSO study found that:

- Most cases of fraudulent financial reporting during the 2000s occurred when companies were experiencing net losses or were in close to break-even positions in periods before the fraud.
- The most common motivations for frauds among public companies included the need to meet earnings expectations, as well as attempts to conceal the company's deteriorating financial condition, increase the stock price, bolster financial performance for pending equity or debt financing, or increase management compensation based on financial results.

The COSO report concluded that additional skepticism is needed at times when there are increased pressures for fraud. These findings reinforce the need for thorough independent audits and candid discussion with auditors of any observations and recommendations.

Financial Results and Likelihood of Fraudulent Reporting



The prospects for convergence with IFRS may compound the challenges that lie ahead, Because IFRS are generally viewed as "principles-based" and less rule-intensive than US GAAP, some believe the added flexibility afforded by IFRS may contribute to a higher likelihood of fraudulent financial reporting and the need for even more judgment by preparers and greater skepticism by independent auditors. The SEC has agreed to conduct a thorough study of the implications before making any final decisions regarding use of IFRS by US issuers. Audit committees and others charged with governance will need to monitor this area closely to identify, monitor and mitigate the risks involved.

Additional information about the COSO study is available in the following report:

- COSO, "Fraudulent Financial Reporting: 1998-2007, An Analysis of U.S. Public Companies," May 2010 (available at **http://www.coso.org/documents/COSOFRAUDSTUDY2010_001.pdf**)

Questions to Ask About Compliance and Financial Reporting

The following questions may be helpful in determining how well your company is coming to grips with risks related to compliance and financial reporting.

1. Has the company evaluated the impact of convergence with IFRS on its internal control systems and financial statements?
2. Is the company monitoring requirements and best practices for disclosures about risks, both in the notes to the financial statements and in other places, including the MD&A sections of annual reports, if applicable?
3. Does the company have a whistleblower program subject to oversight by the audit committee (or others charged with governance)?
4. Has the audit committee (or others charged with governance) approved quantified risk tolerances, where appropriate?

5. Does the audit committee (or others charged with governance) probe the level of risk or uncertainty in critical accounting estimates and discuss the estimates with the external auditor?
6. Is the company's risk management program integrated with its internal and external audits?
7. Have appropriate legal and risk experts been consulted to ensure that all viable risk options have been identified and are appropriately understood?
8. Does the company have risk performance measures to see how well it is managing its risks?
9. Does the company monitor new laws, rules, regulations and accounting changes regularly and update its risk assessments to ensure they remain current?

The Emerging Frontiers of Risk Management

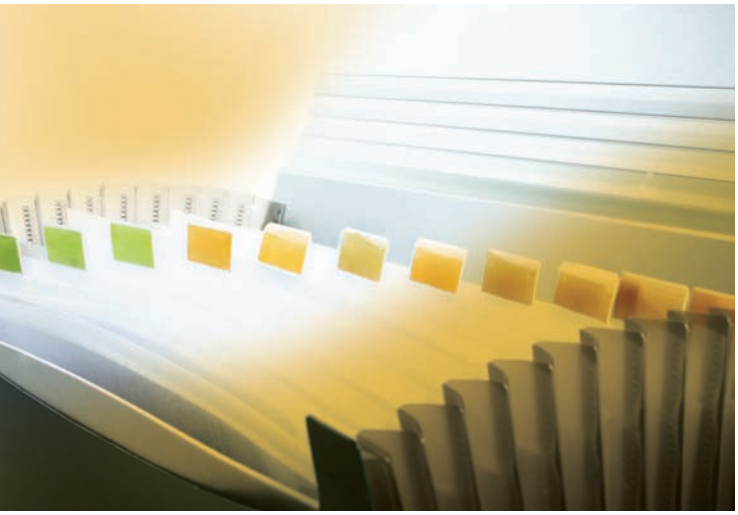
EMERGING RISKS AND KEY RISK INDICATORS

Ultimately, the goal of any risk management program is to enable management to take action in time to mitigate the risks and avoid harm to the company's reputation, assets, and value. Yet many companies seem to be struggling with the identification and reporting phases, leaving business owners and boards of directors dissatisfied with the results. Common frustrations include the time and cost requirements, as well as the degree of difficulty involved in aggregating risks to come up with some sort of bottom line indicator that is helpful to boards. Through a series of surveys and white papers, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) and other groups are advocating a number of steps to help overcome these frustrations and take enterprise risk management (ERM) to the next level.

Risk Reporting: Areas for Improvement

Recent surveys have honed in on the specific areas of improvement that are of the most interest to corporate boards of directors. Most notably, boards want regular and robust systems of reporting risks and they want managers to become more involved in enterprise risk management processes that cover the entire company, not just selected business operations. Here are a few examples of recent findings that reflect these wants and needs:

- COSO sponsored a survey of CFOs in the AICPA's business and industry group in 2008. The survey found that boards of directors were asking senior executives to increase their involvement in risk oversight in almost half the organizations represented.
- The study of the AICPA group also found there was no formal enterprise-wide risk management process in place at a significant minority (44%) of the companies surveyed, and fully 75% of the companies surveyed said that key risks were communicated only on an ad hoc basis at management meetings.
- A more recent COSO study released in 2010 found that very few companies (28%) describe their ERM systems as "systematic, robust and repeatable," while fully 60% of the companies surveyed described their risk taking as mostly informal or tracked only within individual silos rather than enterprise-wide.



- The majority (almost two-thirds) of the companies in the 2010 survey say they report top risk exposures to the board on a regularly-scheduled basis. However, the form of oversight appears to be casual and unstructured.

Challenges: Emerging Risks and Measurements of Intangibles

Why are risk management reporting systems falling short of expectations? Arguably the most difficult obstacles to systematic, robust, and repeatable risk management processes today involve:

1. Maintaining a system that keeps up to date with emerging risks, rather than simply rolling forward and updating the ones identified in prior years, and
2. Developing practical, cost-effective systems of reporting risks related to difficult-to-measure intangibles, such as the security of a company's data, or the quality of its financial reporting practices.

Techniques

While intangibles remain difficult to measure, several techniques have been developed to help overcome the obstacles related to reporting systems. Brief summaries of the suggested approaches are as follows:

- **Leading risk indicators and escalation triggers.** The COSO's 2004 report suggests the use of leading risk indicators and escalation or threshold triggers.

  Examples: A company might monitor consumer confidence as a leading indicator of sales volume (projected units sold per store per month). Or it might monitor an index of staff morale of high performers as a leading indicator of staff turnover. The principle behind this approach is that consumer confidence indicators should be reported to boards if they fall short of a pre-determined level; similarly, staff morale indicators should be reported if they fall short of a minimally-acceptable level. In effect, the pre-determined levels are escalation thresholds or risk thresholds. In practice, however, it can be a challenge to agree on meaningful numerical indicators and thresholds.

- **Indicators based on causal analysis.** A 2010 COSO white paper suggests a systematic approach to the development of key risk indicators (KRIs). Under this approach, the selection of KRIs is based on an analysis of the root causes of events indentified as significant.

  Examples: A company might identify a broken debt covenant as a significant event that should be reported to the board of directors. It will likely be difficult to identify a single root cause for a broken covenant. But an analysis of possible causes might lead to the identification of intermediate factors, such as decreases in sales in recent months or shortages of cash resulting in the need for short-term borrowing. These factors in turn might result from overall economic conditions, pricing trends, or labor issues – and these factors would be seen as the root causes for which key risk indicators should be developed.

Because the 2010 approach considers it unlikely that any one indicator will adequately capture all the facets of a developing risk, a corollary principle is that most companies will need to monitor and weight a dashboard of indicators.

Illustration: Dashboard of Indicators

For some companies, the best approach may be a risk scorecard that uses a combination of the two techniques described above by reporting on the intangibles at risk without trying to measure them. This can be done using KRIs, color-coded status indicators, and an arrow to show the trend, (i.e., whether the risk is increasing or decreasing) as illustrated in the table on the next page.

In effect, the color-coded icons in the table reflect the positioning of the risk on a risk map or heat map. Green represents risks that are low impact and have a low likelihood of happening; red represents risks that would have a high impact and a high likelihood of materializing; and amber represents risks that are medium impact and have a moderate chance of happening. The arrows indicate whether the risk to the assets is increasing or decreasing. For example, a downward trend in the number of known vulnerabilities to hacker attacks is an indication that the company's data security risk is decreasing, while an upward

trend in the number of non-US finance directors who are not knowledgeable about US GAAP is an indication that risk to the quality of the company's financial reporting under US GAAP is increasing.

Assets at Risk	Key Risk Indicators	Status	Trend
Security of customer data	Known vulnerabilities	●	⇩
	Number of unauthorized attempts to access data	●	⇩
Company's reputation for safety	Spills of hazardous materials transported by company	●	⇧
	No. of workplace accidents	●	—
Quality of financial reporting	No. of incidents of fraudulent reporting called into the hotline	●	—
	No. of non-US subsidiaries with finance directors who are not knowledgeable about US GAAP	●	⇧

This approach works well for many types of business risks. But it is difficult to apply to "black swan" risks that are high impact, hard-to-predict risks of events that go beyond the realm of normal expectations in science, finance and technology. Processes for managing these types of risks are still being discussed by managers, risk advisors, and academics.

For More Information

The following materials are referenced in this report and available at **www.coso.org**:

- COSO, Enterprise Risk Management — Integrated Framework, 2004
- Report on the Current State of Enterprise Risk Oversight, Management Accounting Research Conducted on Behalf of the AICPA, Mark Beasley, Bruce Branson, and Bonnie Hancock, 2009

- Developing Key Risk Indicators to Strengthen Enterprise Risk Management: How Key Risk Indicators Can Sharpen Focus on Emerging Risks, COSO, Mark Beasley, Bruce C. Branson, and Bonnie Hancock
- COSO's 2010 Report on ERM: Current State of Enterprise Risk Oversight and Market Perceptions of COSO's ERM Framework, 2010

How We Can Help

At CBIZ, we have always viewed adoption of ERM as a journey rather than an event. Our vision for the future is a level playing field where enterprises of all sizes and in all industries have the kinds of practical and flexible tools needed for successful risk management. By that we mean the kinds of cost-effective tools that will allow management to identify, monitor, and mitigate risks successfully. Our risk advisory services and publications are designed to help make this vision a reality. In addition to enterprise risk management services, we provide a full range of risk advisory services including the following: internal audit services, fraud investigations, proactive anti-fraud programs, IT audit and security services, service organization reporting (formerly known as SAS 70 services), business continuity planning, and IPO audit support.

If you have questions about this report or how to apply the insights to your organization, please contact Michael Gallagher or Brian Gregory.

CBIZ Risk & Advisory Services

Your independent resource for a broad range of risk management and business advisory services.

Visit our website at **http://www.cbiz.com/ras/**
Download our Risk & Advisory Services Brochure.

CBIZ MHM is the brand name for CBIZ MHM, LLC and other Financial Services subsidiaries of CBIZ, Inc. (NYSE: CBZ) that provide tax, financial advisory and consulting services to individuals, tax-exempt organizations and a wide range of publicly-traded and privately-held companies.

Contacts

Brian Gregory
President and Senior Managing Director
CBIZ MHM
Risk and Advisory Services
bgregory@cbiz.com
216.525.1954

Michael S. Gallagher
Managing Director
CBIZ MHM
Enterprise Risk
Management Services
mgallagher@cbiz.com
713.562.1154