McGladrey

Insights for Governance and Growth

TABLE OF CONTENTS

A Message from Joe Adams

Every week I speak with clients and other middle-market business leaders about what it takes to be successful in today's complex marketplace. While it's an ever-evolving conversation, I'm pleased to share with you this special supplement featuring the latest insights from some of McGladrey's thought leaders. The topics featured in these articles—Dodd-Frank, cloud computing, enterprise risk management, security and privacy—are just a handful of the issues we've heard that you and your representative companies are diligently working to address.

One of the core promises McGladrey makes to each of its clients is to truly understand their goals and provide quality services to help them achieve their business strategies within the public trust framework. Delivering on this promise requires sharing our specialized perspectives, particularly with small and mid-size organizations that typically have more limited resources to address business opportunities and challenges. In that spirit, we are honored to have established a strong partnership with the National Association of Corporate Directors to help these organizations address critical issues. We look forward to collaborating with the NACD to bring you the latest thinking through *NACD Directorship*, online features and at the annual NACD Board Leadership conference this October in Washington, D.C.

I hope you find the McGladrey insights in this supplement useful. If you would like to learn more about how McGladrey can advise and assist your organization, please visit www.mcgladrey.com/corporategovernance or reach out to me directly at joe.adams@mcgladrey.com.

Best regards,

Joe Adams

Joseph M. Adams
Managing Partner & CEO
McGladrey LLP
joe.adams@mcgladrey.com

PERSPECTIVE

A Conversation with Phyllis Deiso

Phyllis Deiso leads McGladrey LLP's National SEC Practice, managing the firm's client service and growth initiatives for public companies. She also serves as the lead audit partner for several of the firm's largest clients. For some 20 years, Deiso has worked closely with boards and management on a wide range of complex transaction and financial reporting matters. She joined McGladrey in 2006 after 14 years with a Big Four accounting firm.

What are the biggest issues facing your clients today?

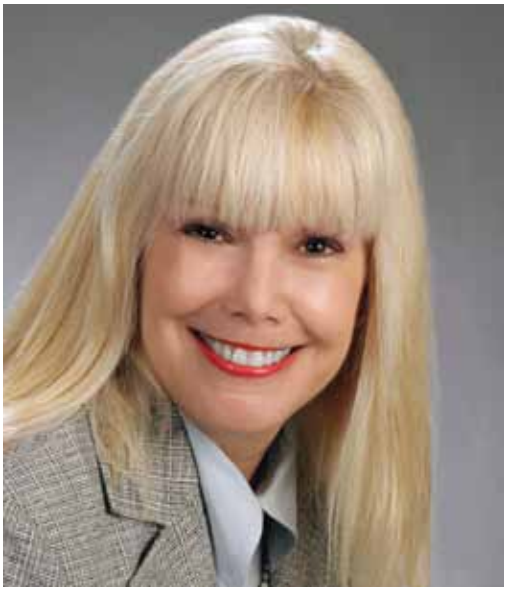
One word sums it up: complexity. From an accounting and financial reporting perspective, the past decade has introduced a significant amount of new regulation. Add to this shareholders' heightened expectations around enterprise risk management and fiduciary accountability. For the middle-market organizations I work with, I see these challenges as being even more acute. Often this constituency has limited internal resources, and the capacity necessary to implement complex standards and regulations is not always available.

What should board members look for in an auditor?

Basic qualifications such as relevant industry knowledge and experience serving public companies should be there, of course. Beyond that, it's very important to understand the audit firm's philosophy for working with its clients and to feel confident the audit firm can operate within the organization's culture. There are some key questions the audit committee can ask: How will the audit firm handle difficult questions when they arise? Every firm has consultations with their national offices, but to what extent are partners empowered to make decisions in the field? I tell people to look at leverage. What is the partner-to-staff ratio working on your engagement? Our experience is that a greater degree of partner-level involvement usually translates into a more efficient audit and a mutually beneficial experience.

Fraud is a burning issue for boards. How do you see the auditor's role as "professional skeptic" helping to address this issue?

By strict definition, our job as auditors is not to uncover fraud. That said, the work auditors perform can play a role in determining those scenarios where fraud has a higher likelihood of occurring. In these instances, communication between the audit committee and the audit firm is paramount. Like any firm, we will only associate with the companies and management teams we trust have integrity. But that trust doesn't excuse us from asking tough questions.



What should a company do when it decides to enter into an IPO?

If a company is considering any type of transaction, it's important to prepare for the process well in advance by looking, for example, at their corporate governance and financial reporting. This could mean establishing an audit committee, tightening internal controls and preparing quarterly financial statements as if the organization is already public. Some of these things are not immediately required upon the close of an IPO, but underwriters have more confidence when they know you have this discipline in place. We have found that middle-market companies appreciate having an external accountant who knows the ins and outs of going public and can provide the necessary guidance well in advance of the offering.

What advice would you give audit committees and boards regarding risk management?

Understandably, boards are very concerned about risk management and their responsibility to shareholders. We live in a complex business environment, and boards face escalating fiduciary expectations. Many types of risks face organizations today, financial and operational among them. While the audit committee is responsible for financial reporting risk, they have to understand the operational challenges too. Definitions of board responsibilities, as they relate to audit committee responsibilities, should be very clear. This ensures that enterprise risk is fully addressed.

ERM: The Board's Role in Corporate Governance

By John Brackett

John Brackett is a partner with McGladrey LLP, where he leads the firm's national Enterprise Risk Management practice. He can be reached at john.brackett@mcgladrey.com.

An effective risk management framework is critical to the sustainability of companies of all sizes and structures. Taking on some level of risk is imperative to executing a successful business strategy. In the midst of the financial crisis and various corporate scandals, the skepticism and scrutiny coming from regulators and investors continue to grow. As a result, enterprise risk management is now seen as a necessity rather than an option for developing and executing an effective growth plan. Yet, according to NACD's *2011 Public Company Governance Survey*, only half of the companies surveyed have operational ERM programs in place today.

For board members who are not confident their companies have adequate programs in place, where to begin? Not all organizations are the same; there is no one-size-fits-all ERM solution or time frame for creating a manageable program. The following four-phase methodology, however, can help companies address the core components of risk and establish a framework that reflects the company's specific needs.

Phase 1: Risk Program Development

Priority is given to the design and development of the ERM strategy and program. Identification of the key personnel who will be involved in program oversight is established at both the board and management levels. Additionally, an assessment of tone at the top, risk appetite, risk materiality, and the tools and templates necessary to manage the program is conducted.

Phase 2: Risk Prioritization

Identifying and documenting the organization's portfolio of risks are the focus of phase two. The tasks may vary, but traditionally they include:

- Evaluating all key functional areas and benchmarking them against available risk universes or libraries
- Categorizing risks within the ERM Integrated Committee of Sponsoring Organizations of the Treadway Commission (COSO) elements of strategy, operations and compliance
- Ranking and prioritizing the identified risks according to impact and likelihood

This phase also includes regular meetings with key personnel to review various categorizations and prioritizations, ensuring a common understanding of scope and systemic risks.

Phase 3: Risk Treatment

The third phase of implementation includes discussing and identifying mitigation strategies for the prioritized risks and defining the organization's risk appetite and tolerance. Additionally, control gaps or improvement opportunities are documented.

Phase 4: Risk Validation and Monitoring

Validation is completed using a variety of assessment options, including self-assessment, internal audit and third-party assistance. The key to this phase is the effective design of a validation plan that verifies that mitigation strategies are working. Additionally, an ongoing monitoring and reporting strategy, such as a board-level dashboard, is developed.

Two trends that illustrate the importance organizations and their boards are placing on ERM are the establishment of risk committees and the naming of chief risk officers (CROs). While every board member has responsibility for risk oversight, risk committees present an opportunity to bring more continuity to the way risk identification, assessment, mitigation and monitoring are handled.

CROs can establish clarity around who "owns" the day-to-day ERM process, though today they are rarely seen outside of highly regulated industries such as financial services and energy. Independence and an ability to facilitate a "no surprises" environment are important characteristics in a CRO's function. In most cases, the CRO will have a dual reporting structure that ensures the appropriate interactions with executive management and the board simultaneously. The level of independence the CRO maintains can boost the confidence the board has in the ERM program.

The board's role of providing proper oversight is best accomplished when risk is woven into every discussion and not set aside and addressed as a discrete activity. An effective, pragmatic ERM program can drive risk awareness throughout the organization and can help fulfill the board's responsibilities to all stakeholders. Best of all, implementation and ongoing management don't need to be onerous. So while you can't operate or grow a business without risk, a robust ERM program definitely can help minimize unnecessary business disruptions.

The Important Risks of Cloud Computing

By Daimon Geopfert

Daimon Geopfert is the national leader for security and privacy consulting at McGladrey LLP. He can be reached at daimon.geopfert@mcgladrey.com.

Cloud computing has become a popular solution for organizations to house technology operations, software and data. It is perceived as more cost-effective than in-house solutions, reducing expenditures related to infrastructure, staff and software, while also being safer than traditional internal solutions. While management is responsible for making decisions about technology and its related costs, the board must be involved in the development of a cloud strategy, as potentially significant risks exist that could have dangerous consequences for the company.

Cloud solutions are an excellent option for many organizations, but some business processes simply may not be appropriate for the cloud due to risk and regulatory concerns. Some companies have suffered by migrating to the cloud too quickly, without fully understanding the risks involved. For those organizations that could benefit from cloud solutions, there is no one-size-fits-all answer, with a wide variety of options available in the marketplace. Therefore, the board should play an integral part in determining the most beneficial strategy for the security, privacy and regulatory needs of the company and avoiding unplanned costs.

Depending on the demands of the company, there are two distinct categories of cloud solutions: public and private. In the public cloud, applications and data are hosted for a wide variety of customers at once. This is the more cost-effective option, but it may not meet the needs of companies with complex security or regulatory responsibilities.

Larger organizations with more significant storage and compliance demands are prime candidates for private clouds. These dedicated storage solutions offer more control over data, access, auditing and reporting in a closed environment, but are significantly less cost-efficient. Another issue is that these solutions are sometimes tied to legacy systems and can inherit existing security concerns.

If cost were the sole consideration, the public cloud would be the optimal choice. However, management must be cognizant of regulatory, security and privacy concerns along with the financial aspect of cloud solutions. As widespread as cloud computing has become, there still may be situations where a company's unique needs simply are not a fit for its inherent limitations. In their oversight role, board members must ensure that management is evaluating the potentially substantial risks that could be introduced to the company.

Security and Privacy

A critical factor for boards to understand when developing a cloud strategy is that the cloud is not always safer than an in-house system. The cloud comes with its own unique risks, and it may not be in the company's best interest to trade one type of risk for another. While systems are technically more secure in a cloud environment, moving applications could create new regulatory and legal concerns. While clouds likely come with a higher level of security than legacy servers, as they become more popular they also become a more attractive target for hackers. The probability of an attack is relatively low, but even if only one is successful, the impact could be significant.

Compliance Issues

A host of IT compliance issues arise when a company decides to migrate to the cloud. These are often industry-specific regulatory issues, such as Payment Card Industry (PCI), Health Insurance Portability and Accountability Act (HIPAA) and Financial Industry Regulatory Authority (FINRA). Regulations that could impact cloud solutions are constantly changing, so it is advised that a company consult with qualified legal counsel and its internal audit functions prior to deploying a cloud strategy.

Hidden Costs

Normally, the board would not be concerned with budgeting, as this falls under the purview of management. However, board directors should exercise risk oversight to ask management about possible hidden costs, such as whether business processes will be disrupted by a potential cloud solution, and whether special audits or regulatory reviews could disturb normal operations. The board must ensure that these risks are being managed properly to avoid potential financial damage to the company resulting from a reduction in productivity or regulatory sanctions.

With the increasing popularity of cloud computing and the significant cost savings that can be realized, the risks that come along with these solutions are sometimes ignored. With the board's role of due diligence and risk oversight, it is critical to ensure that management has taken these risk factors into account when evaluating which, if any, cloud solution is suitable for the organization.

Pressing Issues for Mid-Size Company Boards

McGladrey LLP, together with the National Association of Corporate Directors, has produced a series of videos about some of the most pressing issues facing mid-size companies today. Drawing on their history of advising boards of middle-market companies, McGladrey specialists share valuable insights on the crucial points directors should consider.

Following are highlights of the four most recent videos. Find them online at NACDonline.org/boardvision.

Every Board's Responsibility: Oversight of Enterprise Risk Management

With John Brackett, McGladrey partner and enterprise risk management practice leader

While enterprise risk management is widely seen as a critical strategic component for all companies to achieve sustainability and growth, only half of those participating in the NACD's *2011 Public Company Governance Survey* have ERM programs in place. It is the board's responsibility to ensure a program is operational and that it addresses the company's most important issues.

In this NACD *BoardVision* episode, McGladrey partner John Brackett discusses issues board members should keep in mind, including:

- Three areas in which a director's personal or professional experiences are particularly invaluable
- The emergence of risk committees and chief risk officers
- Key strategies that boards should consider in order to optimize their risk oversight responsibilities

IT Security Failures: Prepare to Detect and Handle an IT Crisis

With Daimon Geopfert, McGladrey national leader for IT security and privacy consulting

Most companies—and their boards—focus on preventing IT security incidents at the expense of attack detection and correction. Perpetrators of IT attacks are more sophisticated than ever, so board members should establish comprehensive plans based on the assumption that their company's preventive controls will fail at some point.

In this NACD *BoardVision* episode, McGladrey director Daimon Geopfert discusses response plans for IT failures, covering:

- The critical questions board members should ask their CIO and IT leadership
- The structure of modern attack methods
- The features of a realistic, well-designed security risk process
- The best ways board members can leverage their crisis management experience in the event of a breach.

Blue Skies for Cloud Computing: Addressing Security and Privacy

With Daimon Geopfert, McGladrey national leader for IT security and privacy consulting

Moving computer operations into "the cloud" can promise cost savings in IT infrastructure, software and staff while providing a more secure IT environment. Many organizations may press ahead on this tempting prospect without fully understanding the underlying risks. This is when risk oversight by a company's board becomes paramount.

In this edition of NACD *BoardVision*, McGladrey director Daimon Geopfert discusses the security and privacy concerns of cloud computing, along with boardroom strategies for the new computing future. He addresses:

- How security and privacy risks, regulatory impact and hidden costs affect board oversight
- The trade-offs in regulatory and legal risks when transitioning to a cloud-based environment
- The pros and cons of outsourcing to the cloud
- The differences between public and private clouds

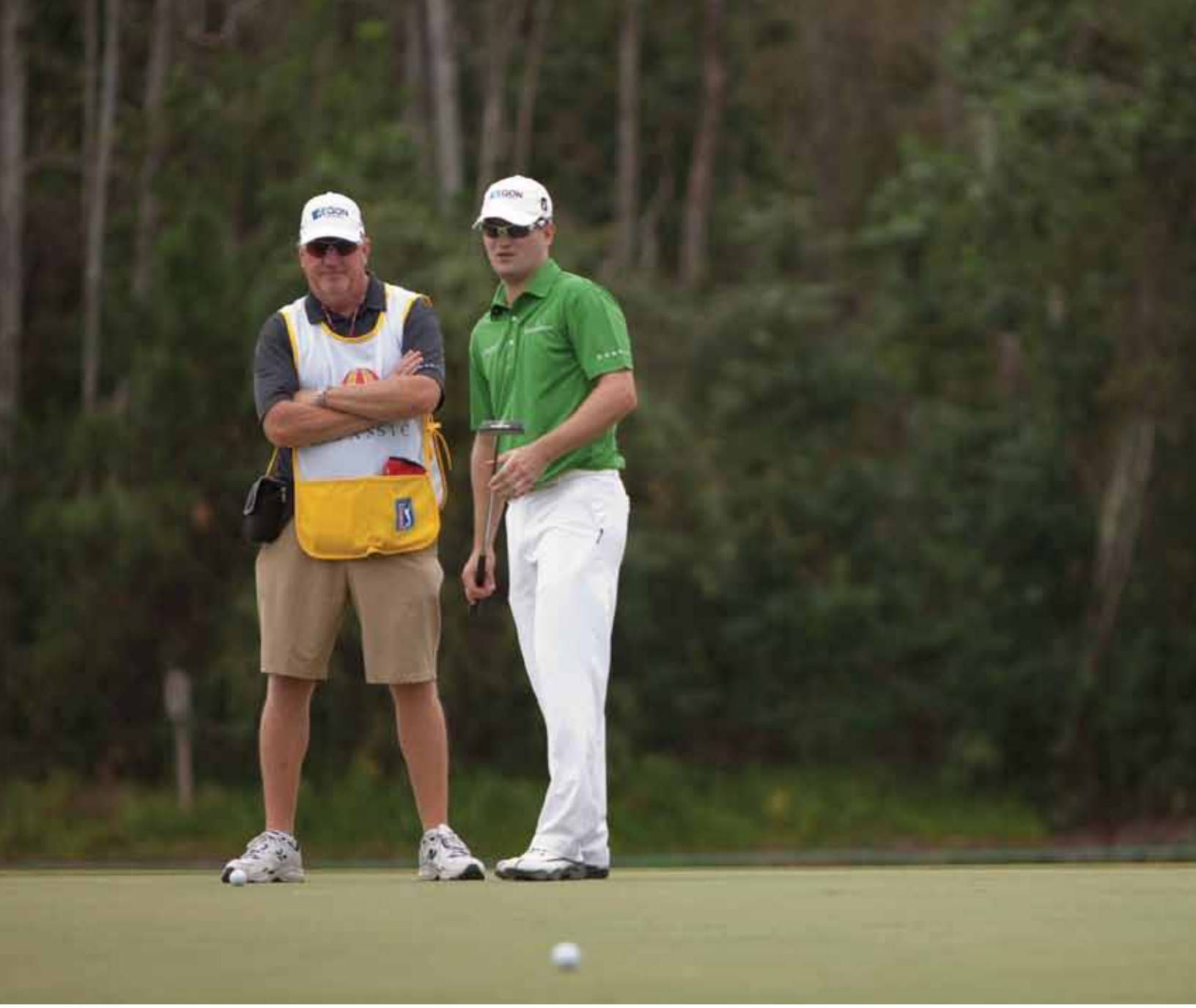
Watch these informative videos at www.nacdonline.org/BoardVision

The Top Governance Issues Facing Mid-Size Public Companies

With Phyllis Deiso, McGladrey national SEC practice leader

Small and mid-size public companies face the same complex regulatory and business environments as large multinationals, but must often make do with fewer resources. In this interview with *NACD Directorship* magazine, McGladrey national SEC practice leader Phyllis Deiso offers insights on some of the top governance issues facing today's mid-size corporate directors, including:

- How a board should comply with whistleblower rules and encourage internal reporting before the whistleblower goes to the SEC
- Corporate provisions of Dodd-Frank regarding annual shareholder assessment of say on pay
- Best practices for the board or audit committee for interacting with the company's external accountant



Power comes from being understood.SM

When you trust the advice you're getting, you know your next move is the right move. That's what you can expect from McGladrey. That's the power of being understood.

To learn how we can help your organization, call 800.274.3978.

Experience the power
Go to www.mcgladrey.com

McGladrey

Assurance ▪ Tax ▪ Consulting

Power comes from being understood.[SM]

When you trust the advice you're getting, you know your next move is the right move. That's what you can expect from McGladrey. That's the power of being understood.

www.mcgladrey.com

About McGladrey

McGladrey LLP is the fifth-largest U.S. provider of assurance, tax and consulting services, with nearly 6,500 professionals and associates in more than 70 offices nationwide. McGladrey is a licensed CPA firm and a member of RSM International, the sixth-largest global network of independent accounting, tax and consulting firms.

McGladrey

To learn more, contact Partner Phyllis Deiso at 954.356.5759
or phyllis.deiso@mcgladrey.com.