



The Compliance Journey

Making Compliance Sustainable

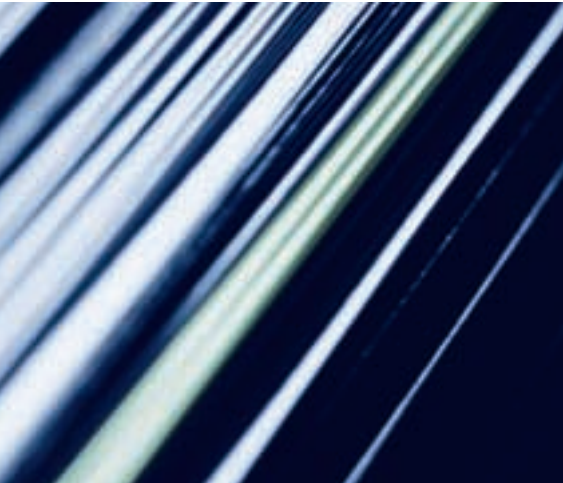
ADVISORY

AUDIT ■ TAX ■ ADVISORY

© 2005 KPMG International. KPMG International is a Swiss cooperative of which all KPMG firms are members. KPMG International provides no services to clients. Each member firm is a separate and independent legal entity and each describes itself as such. All rights reserved.



Introduction



As the initial year for compliance with section 404 of the Sarbanes-Oxley Act of 2002¹ draws to a close, many leaders are beginning to reflect on the considerable effort their organizations undertook to achieve initial compliance.

Apart from the sizeable commitment of financial resources necessary, the effort to comply with section 404² and other key sections of the Act also has required the time and attention of numerous employees, many of whom were asked to delay work on other projects to meet compliance requirements.

Now, many leaders are beginning to think about year two—and all future years—when they must test, report, and certify internal control over financial reporting on an ongoing basis. They recognize that the intense, costly, project-oriented focus that prevailed in year one is likely inappropriate and unsustainable over time. At the same time, many of them acknowledge that the intensity of their organizations' focus on the issue is likely to diminish once deadlines pass and new priorities emerge. Consequently, they know they risk the erosion of first-year efforts if they do not find a way to sustain ongoing compliance effectively.

Concern about maintaining and evolving compliance efforts is widespread. A survey conducted in September 2004 among 530 public companies by KPMG's 404 Institute indicated that as many as 70 percent of organizations had not begun, or were just beginning, the planning efforts needed to maintain ongoing compliance.³ In the process they had identified major challenges that could impede their progress. Their experience indicates that over time, compliance must evolve to become business as usual. Compliance and business processes will be fundamentally aligned so controls and reporting will naturally evolve as the business changes. This evolution is critical—and not just because effective leaders want to use scarce resources efficiently and preserve the benefits derived from initial compliance. This evolution is also important because leaders understand the fundamental value of improved transparency and bolstered investor and market confidence that the Act helps enable.

KPMG's first paper in this series, *The Compliance Journey: Balancing Risk and Controls with Performance Improvement*, considered how organizations are transforming their controls so that they are embedded in the business and how compliance can enable performance improvement. This document continues that discussion with a focus on ongoing compliance. It describes how organizations' efforts to sustain compliance can progress along four states of compliance to ultimately reduce both risk and cost.

This endeavor should be among organizations' most significant priorities today. Getting it right, however, is not an end-state but an evolution. In the years to come, an organization's ongoing compliance efforts will change and mature, in keeping with other changes in its business environment and its need to create value. Over time, those efforts will help reduce the costs and risks associated with compliance. This document describes a model that can provide leaders with a means of evaluating their organizations to determine how they want their ongoing compliance efforts to evolve.

¹ Sarbanes-Oxley or the Act.

² Section 404 requires that management document and assess internal control over financial reporting, report on the assessment, and subject the assessment to audit by the organization's independent auditor.

³ KPMG's 404 Institute, Second Web survey, KPMG LLP, 2004.

The Current Environment

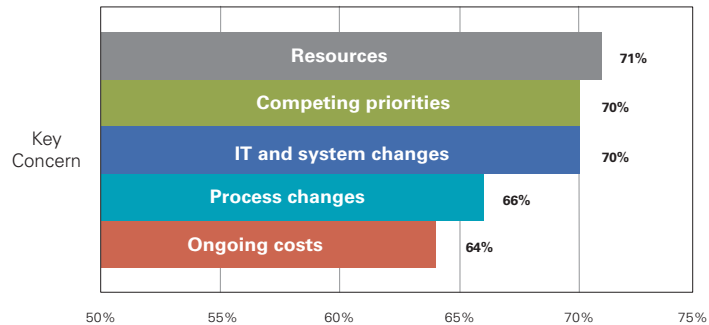


For many organizations, meeting the section 404 deadline has been challenging. Few businesses are organized to readily accommodate the changes required for compliance. A survey conducted among 530 public companies in September 2004 by KPMG's 404 Institute found, for example, that more than half of those surveyed anticipated completing the evaluation and testing phases within two months of the end of their fiscal years.⁴

Most respondents to KPMG's survey noted that they started section 404 compliance with a resource-intensive, project approach. Now, in considering ongoing compliance, many are beginning to identify major challenges to their initial approach (see *Figure 1*).

Figure 1: Top Challenges of Ongoing Compliance

Survey participants who are actively engaged in or responsible for compliance with section 404 have a number of key concerns:



Percentage of survey participants actively engaged in or responsible for compliance with section 404.

Source: KPMG's 404 Institute, 2004.

Analysts and the media have often focused on the cost of section 404 documentation, testing, and attestation. Fortune 1000 companies have spent or will spend millions of dollars to comply with the Act. But KPMG's recent survey shows that the primary concern of the respondents was resource constraints. The effects of resource constraints include:

- **Many companies expect to complete initial compliance within weeks of their deadlines.** Despite considerable dedication of resources to the effort, the project took longer than expected, leaving very little time to complete their assessment requirements and then plan or evolve their compliance efforts.
- **Leaders recognize that they must find a way to sustain ongoing compliance effectively and efficiently.** The intense, costly, project-oriented focus that prevailed in year one is likely inappropriate and unsustainable over time.

⁴ KPMG's 404 Institute, Second Web survey, KPMG LLP, 2004.

A closely related constraint is competing priorities.

- **Many important projects were delayed to free up the necessary resources to meet compliance requirements.** Aside from the sizable commitment of financial resources necessary, the effort to comply with section 404 and other key sections of the Act also has required the time and attention of numerous employees, many of whom were pulled from work on other important projects.
- **Many companies acknowledge that the intensity of their compliance efforts is likely to diminish.** Once deadlines pass and new business requirements emerge, organizations will likely set new priorities, thereby risking the erosion of first-year efforts and sub-optimizing further compliance efforts.

Other constraints are the result of business, system, and IT changes. Most business organizations evolve continuously, and the processes that support compliance must evolve efficiently in alignment with the business changes. For example:

- **The natural growth and expansion of a healthy business often introduces new business processes.** These new business processes add to the requirements for controls, reporting, and attestation. They must be accommodated on a timely basis and fully integrated into the overall controls architecture.
- **The reinvention of businesses must be complemented by appropriate adjustments in compliance processes.** Businesses must continuously evolve their operating assets to address new business conditions and technological advancements. The means to achieve compliance and the very nature of compliance must evolve with these changes.

These findings indicate that, as with other business goals and challenges, organizations need to find ways to achieve ongoing compliance more efficiently and effectively over time.

Understanding Ongoing Compliance Risk and Cost



Like other business endeavors, ongoing compliance with section 404 poses specific risks and costs that organizations must manage.

As KPMG's research and experience have shown, addressing such issues requires considerable financial and human resources. Inadequate investments could put the effort at risk of failure. While the cost of compliance appears high, the cost of failure is unaffordable. Balancing cost and risk, therefore, can pay off throughout the business.

Compliance Risks and Their Potential Consequences

Risk	Potential Consequences
Reduced Market Confidence	<ul style="list-style-type: none"> • Degradation in debt rating • Higher directors' and officers' insurance premiums and reduction in insurance coverage • Lessened ability to attract board members and potential suitors
Reduced Investor Confidence	<ul style="list-style-type: none"> • Decreased market capitalization • Eroded demand for equities • Decreased analysts' ratings
Reduced Business Performance	<ul style="list-style-type: none"> • Increased management focus on compliance issues vs. business opportunities • Increased attrition and turnover • Decreased ability to attract talent

Source: KPMG LLP (U.S.), 2005.

For purposes of this discussion, the overall cost of ongoing compliance includes those people and infrastructure costs required to document, maintain, test, and report on internal control over financial reporting.⁵

Risks and Costs Evolve as Compliance Matures

Ongoing compliance can be expected to evolve over time. The need for business efficiency, for example, may drive standardization in compliance policies, procedures, definitions, and reporting as well as an increasingly focused monitoring capability. Risk and cost are likely to remain high at the outset of ongoing compliance activities—due to the creation of an overarching compliance function and the additional people, infrastructure, and technology it would require—but then should fall and ultimately converge as ongoing compliance becomes more effective and efficiencies are realized over time. This convergence is indicative of a prudent balance between risk and cost.

⁵ Total cost of control is defined in KPMG's first paper in this series, *The Compliance Journey: Balancing Risk and Controls with Performance Improvement*.

Understanding the Evolution of Ongoing Compliance

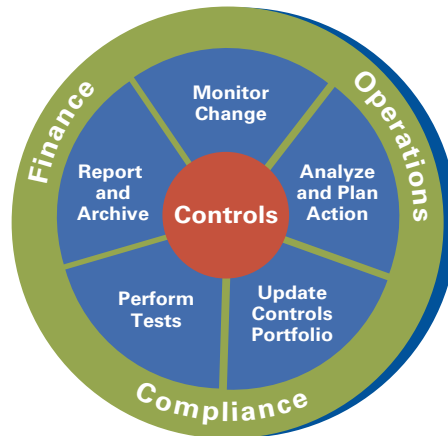


The results of the KPMG survey indicate that ongoing compliance cannot be continuously accommodated by one large-scale project after another. The approach for maintaining compliance—in the face of changing business requirements, technological advancements, and regulatory changes—must be increasingly efficient and sophisticated. The development of such an approach will evolve through several states, as compliance moves from an afterthought to a consideration embedded in every business decision.

Core Activities

The evolution of ongoing compliance begins with understanding the core activities, depicted in *Figure 2* and defined below:

Figure 2: The Components of Compliance in Relation to the Business



As compliance evolves from one state to the next, the performance of each of the five activities, and accountability for their performance, changes within finance, operations, and compliance.

Source: KPMG LLP (U.S.), 2005.

Monitor Change: Capture relevant trigger events that could affect compliance. Such events could include acquisitions, divestitures, IT system implementations, new rules and regulations, significant personnel changes, outsourcing, and entering or exiting markets.

- Identify and capture planned and executed changes to the business
- Monitor changes in rules and regulations
- Determine the changes that have an impact on internal control over financial reporting
- Review period-end results for indications of change not previously identified



Analyze and Plan Action: Analyze triggers of change for action and needed resources.

- Identify controls and processes that are affected
- Assess the impact of change on processes and controls
- Plan resources and timing for implementing changes to processes/controls
- Assign key responsibilities and communicate them

Update Controls Portfolio: Update control/process documentation and implement new controls.

- Design new controls
- Test design effectiveness
- Update process and control documentation
- Assign ownership, train personnel, and implement the new controls
- Retire replaced or legacy controls, as needed

Perform Tests: Create and execute test plans to determine operating effectiveness of internal control over financial reporting.

- Develop test plans, including locations, timing, extent of testing, and resources
- Execute test plans
- Consolidate results of tests and plan remediation as needed
- Prioritize and remediate control gaps

Report and Archive: Analyze, communicate, and certify compliance efforts; archive results for future reference.

- Analyze and categorize test results (i.e., deficiency, significant deficiency, material weakness)
- Communicate results to audit committee, external auditors, and others, as appropriate
- Certify results (as required annually by the Act)
- Archive appropriate documentation for future reference, which could include regulator inquiries

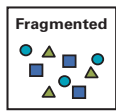
The performance of these activities, and accountability for their performance, occurs within different aspects of the business, including finance, operations, and compliance (see *Figure 2* on page 5). As the process for ongoing compliance evolves, accountability for these activities, as well as who performs them, will change.

How Compliance Evolves Through Four States

The five activities described above constitute an ongoing compliance program. The evolution of such a program can be described as a progression across four key states—fragmented, functional, integrated, and embedded—which are described below. Within each of the four states, organizations will assign accountabilities to leaders, such as a chief compliance officer, chief risk officer, or head of internal audit, who will take ownership for performance of the five ongoing compliance activities.

For example, all four states would include development and execution of test plans. Who develops, executes, and consolidates the results of those test plans will change as the process evolves. Gradually, accountability for the various activities should shift away from Compliance and Finance toward Operations (depicted in the legend at right). Understanding how well the organization performs the ongoing activities in the context of compliance can help leaders assess the organization’s current state—and, ultimately, how it wants to progress. Each organization will determine the pace at which it evolves and matures through the four states of achieving compliance.

The four states are defined as follows:



Fragmented State: Compliance is project-centric. It is achieved through disconnected and/or inconsistently applied efforts throughout the enterprise. Extensive coordination and work are required by a centralized project management function.

During ongoing compliance, leaders would assign accountability to the finance operation and temporarily establish cross-business project teams. The cross-business project teams would:

- Monitor compliance efforts on an ad hoc basis
- Disseminate instructions, templates, and training
- Communicate, perform, and verify tests of internal control over financial reporting



Functional State: Compliance is program-centric. It is achieved via the oversight of a new, overarching, stand-alone program that oversees the hiring of dedicated personnel whose main focus is coordinating and communicating the compliance activities. Such individuals are solely

responsible for the performance of compliance, and they will carry out the activities if necessary.

During ongoing compliance, leaders assign accountability to a centralized compliance office function, such as the chief compliance officer or chief risk officer, and identify process owners. The centralized compliance office function would:

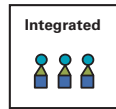
- Implement standard guidance, templates, and training, and consider technology tools to assist in managing the compliance program
- Monitor compliance with routine analysis and reporting
- Communicate, verify, and sometimes perform tests of internal control over financial reporting

Accountabilities Legend

- Finance = ●
- Compliance = ▲
- Operations = ■

Fragmented to Functional

For example, a large conglomerate with decentralized processes and systems had a project-based approach for initial compliance. The initial effort was challenging and resource intensive, with inconsistent policies, procedures, and standards applied across the organization. To move from a “fragmented” to an increasingly “functional” state, management is creating an overarching, stand-alone compliance function, under the accountability of a chief compliance officer. This compliance function will be responsible for coordinating ongoing compliance activities—including establishing policies, procedures, tools, and standards as well as technology enablers—and deploying those throughout the organization. The compliance function will also dedicate resources to helping the business identify changes, execute plans, and monitor compliance.



Integrated State: Compliance is process-centric. It is achieved in a fundamentally new way by building compliance activities and procedures into existing business processes and technology so that business owners can start to share responsibility for compliance. It encompasses a verification and quality assurance role for internal audit (or other centralized compliance functions) to help ensure that compliance is achieved throughout the business.

During ongoing compliance, leaders would assign accountability to process owners, with centralized oversight retained by a compliance function such as the chief compliance officer or chief risk officer. The centralized compliance function would:

- Implement standard guidance, templates, and training, and consider technology solutions to modify current business processes to include compliance requirements
- Monitor compliance with routine analysis and detail reporting from the process owners
- Communicate and periodically verify testing results relating to internal control over financial reporting

Functional to Integrated

For example, a multibillion-dollar retailer recently completed its initial Sarbanes-Oxley compliance program. While the compliance efforts were well managed, they required significant resources, and the compliance function assumed primary accountability for achieving initial compliance. As an outcome of compliance, the company identified significant deficiencies in its centralized IT function. The compliance team experienced numerous challenges in documenting and testing the controls of that function.

Recognizing the significance of these issues, the CIO took ownership of compliance related to IT. As an example of an integrated approach, the CIO focused on building key compliance activities into the system development lifecycle:

- The business case analysis now includes an additional requirement to analyze the impact of proposed system changes on internal controls over financial reporting.
- The design phase now includes the design of new internal controls and design approval by the compliance function.
- The testing and implementation phases now include new requirements to test controls, update documentation, and prepare ongoing test scripts for the new controls.

Based on these changes, the CIO was able to integrate compliance into the system development process, and the company gained additional efficiencies in maintaining compliance.



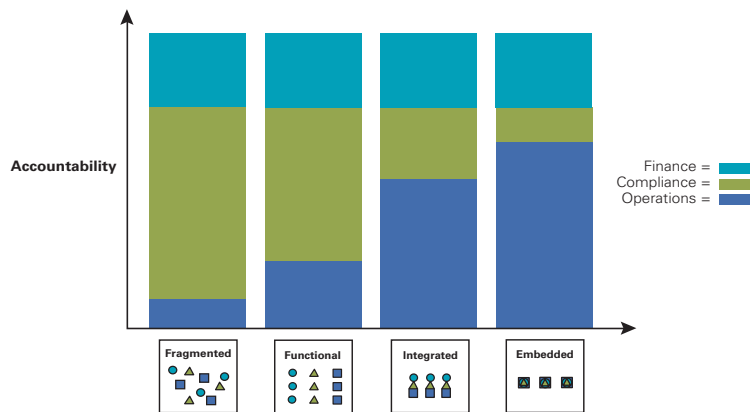
Embedded State: Compliance is culture-centric. It is achieved as part of how business is done and is inherently part of organizational culture. The embedded state implies a change in mindset, in which compliance is performed not solely for the sake of complying with the law but also because it is the right thing to do. Accountability is instilled within the day-to-day actions and responsibilities of every individual. Internal audit, or other compliance functions, provide a quality assurance role to ensure that ongoing compliance is achieved.

During ongoing compliance, leaders would:

- Monitor compliance activities in an ongoing manner inherent to business
- Implement change and refine business practice based on continuous learning
- Communicate the cultural tone, from the top down and bottom up, and reinforce it with compensation and rewards

Over time, an ongoing compliance effort would evolve across this continuum and build off the previous stage. This evolution will drive business benefits as associated risk and cost are reduced. *Figure 3* shows how accountabilities change.

Figure 3: Accountability During the Four States of Compliance



Source: KPMG LLP (U.S.), 2005.

While compliance can be achieved within any of the four states, the process, resources, and related implications will likely vary. What’s more, the speed at which compliance evolves is dependent on the organization’s size, complexity, control environment, and infrastructure. By understanding the four states, an organization can begin to evaluate its current state as well as whether and where it would like to move to the next state.

For example, *Figure 4* illustrates the details of accountability in an example functional state. From these details, an organization can see how different aspects of accountability would change as the organization progresses through the states. (Responsibility for certain activities is shared, as indicated by the placement of more than one check mark.)

Figure 4: Illustrative Accountability Matrix

Roles and Responsibilities	Executive	Finance	Compliance	Business Units/Process Owners	Control Owners
Executive Sponsorship					
Provide executive sponsorship and leadership	✓				
Set the “tone at the top”	✓				
Provide sponsorship and ensure ownership at the business unit level				✓	
Set the “tone at the top” for the business units				✓	
Resolve escalated issues	✓			✓	
Monitor Change					
Identify and capture planned and executed changes to the business			✓		
Monitor changes in rules and regulations			✓		
Determine the changes that have an impact on internal control over financial reporting		✓			
Review period-end results for indications of change not previously identified		✓			
Analyze and Plan Action					
Identify controls and processes that are affected			✓		
Assess the impact of change on processes and controls			✓		
Plan resources and timing for implementation of changes to processes/controls			✓		
Assign key responsibilities and communicate them			✓		
Update Controls Portfolio					
Design new controls			✓	✓	
Test design effectiveness			✓		
Update process and control documentation			✓		
Assign ownership, train personnel, and implement the new controls				✓	
Retire replaced or legacy controls, as needed			✓	✓	
Perform Tests					
Develop test plans, including locations, timing, extent of testing, and resources			✓		
Execute test plans			✓		✓
Consolidate results of tests and plan remediation, as needed			✓		
Prioritize and remediate control gaps			✓	✓	
Report and Analyze					
Analyze and categorize test results			✓		
Communicate results			✓		
Certify results	✓	✓			
Archive appropriate documentation for future reference			✓		

Source: KPMG LLP (U.S.), 2005.

Making Choices



Understanding the key activities of an ongoing compliance process and how those activities evolve over time provides leaders with a variety of choices. To begin to understand the choices and to plan for ongoing compliance, leaders should understand what objectives they want to achieve. Key considerations include:

- Consolidating findings from initial compliance efforts
- Analyzing lessons learned
- Identifying key stakeholders
- Defining accountabilities

An organization’s business and control environments will determine the speed at which it can mature (see key questions below). Once leaders map out where they want to go, they can create a plan for how they want to get there. With a plan in place, leaders can begin to evolve their ongoing compliance program.

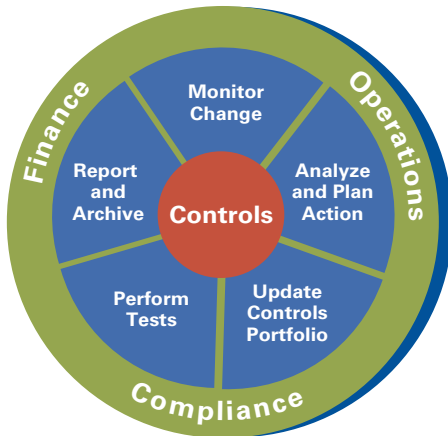
Figure 5: Key Questions to Help Evaluate the State of the Business

Dimension	Key Questions
Process Optimization	<ul style="list-style-type: none"> • How well defined and standardized are organizational processes? • Are back-office functions centralized or decentralized? • How adaptable are processes to handle ongoing changes to the business and related impacts to controls?
Technology	<ul style="list-style-type: none"> • How many key information systems does the organization have, and how reliable are they? • Is the use of technology standardized across organizational processes? • How robust are the organization’s IT governance and system development lifecycle disciplines? • How many interfaces, spreadsheets, and other utilities are used to communicate across the systems?
Organization and People	<ul style="list-style-type: none"> • How complex is the organization’s structure? • Is accountability for controls clearly defined and communicated throughout the organization? • How robust are the organization’s communications, training, and change management capabilities? • How well does the organization handle job transitions and turnover?
Risk and Controls	<ul style="list-style-type: none"> • How many of the organization’s key controls are manual versus automated? • Does the organization have a standard set of controls or are controls determined by function, business, or process?

Source: KPMG LLP (U.S.), 2005.

Conclusion

The Components of Compliance in Relation to the Business



For many organizations, the first year of compliance with Sarbanes-Oxley has been difficult and costly. Most leaders now know that the project-oriented approach that prevailed in year one poses too much risk and cost to be sustainable over time. Many are also realizing that they need to change their approach to ongoing compliance—with all regulations—finding ways to best use their scarce resources to reduce compliance risk and cost over time.

Leaders can facilitate this transformation by seeking to understand how compliance can evolve and what this evolution could mean for their business. They can then address how to make ongoing compliance more efficient and effective. Most organizations are currently in the “fragmented” state, which is to be expected following the challenging work of initial compliance. From that vantage point, the journey to the “embedded” state can seem daunting. Nonetheless, the governance goals of embedded compliance are fundamentally rooted in cultural change—which leaders can begin to address now no matter what state they ultimately decide to pursue. The key to getting started is to focus on the five core activities of ongoing compliance in the context of the compliance states and then to put in place an implementation plan to balance risk and cost over time.

Achieving a balance between risk and cost will take both a concerted effort and a maturing of organizational culture. Alignment of people, processes, and systems, along with the appropriate tone at the top, can help organizations shape ongoing compliance issues as opportunities to relish rather than problems to avoid.

Major KPMG Contributors

Steve Hill
Larry Raff
Tim Flynn
Jack Taylor
Gary Dushane
Carin Abrahamsohn
Christopher Berger
Neil Brigham
Colleen Drummond
Don Farineau
Mark Goodburn
John Kunasek
Carole Law
Mark Lindig
Robert Lipstein
Diane Nardin
Michael Nolan
Joseph Orlando
Gary Riske
John Rittenhouse
Viktor Rzeteljski
Mike Salazar
Ted Senko

Contacts

Steve Hill
KPMG LLP (U.S.)
214-840-4455
shill@kpmg.com

Larry Raff
KPMG LLP (U.S.)
212-872-3387
lraff@kpmg.com

Mark Goodburn
KPMG LLP (U.S.)
212-872-5880
mgoodburn@kpmg.com

Mark Lindig
KPMG LLP (U.S.)
212-872-3889
mtlindig@kpmg.com

Ted Senko
KPMG LLP (U.S.)
303-295-8828
tsenko@kpmg.com

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

Visit KPMG on the World Wide Web at www.kpmg.com.

KPMG International is a Swiss cooperative that serves as a coordinating entity for a network of independent member firms. KPMG International provides no audit or other client services. Such services are provided solely by member firms in their respective geographic areas. KPMG International and its member firms are legally distinct and separate entities. They are not and nothing contained herein shall be construed to place these entities in the relationship of parents, subsidiaries, agents, partners, or joint venturers. No member firm has any authority (actual, apparent, implied or otherwise) to obligate or bind KPMG International or any member firm in any manner whatsoever, or vice versa.

© 2005 KPMG International. KPMG International is a Swiss cooperative of which all KPMG firms are members. KPMG International provides no services to clients. Each member firm is a separate and independent legal entity and each describes itself as such. All rights reserved. Printed in the U.S.A. 27477atl

KPMG and the KPMG logo are registered trademarks of KPMG International.

