Deloitte
& Touche

Meeting the Challenge

How Financial Institutions Are Responding to Sarbanes-Oxley

Serving the Financial Services Industry Globally

Dear Colleague:

We are pleased to provide you with this copy of *Meeting the Challenge - How Financial Institutions Are Responding to Sarbanes-Oxley*. This publication describes the special challenges that the internal control requirements of Sections 302 and 404 pose for companies in the financial services industry, and what well-managed firms are doing in response.

In *Moving Forward - A Guide to Improving Corporate Governance Through Effective Internal Control*, we outline what Sections 302 and 404 require of all public companies in the United States, and recommend a detailed, five-step process for developing an internal control program to address these provisions. The present publication addresses the specific issues faced by banks, securities firms, insurance and asset management companies in developing and implementing their internal control programs. It presents some conclusions, drawn from our own experience and that of client firms, which we believe will be helpful to others in the financial services industry.

As both publications make clear, the Sarbanes-Oxley clock is ticking. Section 302 is already in effect, and Section 404 will take effect later this year, possibly as early as September. The time for effective action is *now*.

We hope you will find them useful and informative.

Sincerely,

William C. Freda
Chairman
Global Financial Services Industry Practice

The Clock is **Ticking**

Section 302 of the Sarbanes-Oxley Act, (the Act), which requires CEOs and CFOs to personally certify that they are responsible for disclosure controls and procedures, is already in force. Section 404 of the Act, which mandates annual evaluation and attestation by the company's independent auditor of internal controls and procedures for financial reporting, is expected to go into effect in late 2003, possibly as early as September. The clock is ticking: even as government agencies scramble to put the regulations in place, the time for companies to gear up for compliance is now.

Financial Services Firms: Well Positioned But Much Remains to Be Done

Because sound management of market, credit and operational risk is so critical to their success, many financial institutions have already devoted substantial resources to internal controls that support their risk management processes, and continue to do so. For the same reasons, many already have effective, highly developed internal audit functions. To varying degrees depending upon the industry segments and, in some instances, the jurisdictions in which they are active, they are also subject to heightened regulation that, in some cases, already parallels the new regulatory environment that Sarbanes-Oxley generally imposes on Corporate America.

Many financial services firms are already relatively well positioned to plan and develop their Sarbanes-Oxley compliance programs. However, much may remain to be done. Mechanisms to ensure alignment between senior management and the audit committee, who make strategic governance decisions and set "the tone at the top," and internal control processes at the operational level may be limited. Control frameworks are often not well documented, inconsistent and not measurable. Existing internal controls rarely address the disclosure controls mandated by Sarbanes-Oxley, and top management may have limited visibility into their effectiveness.

Sarbanes-Oxley compliance will require:

- Creation of a high-level framework that fully integrates corporate governance factors with internal controls
- Adoption of a method that relates financial statement components to critical business cycles and critical controls
- Documentation of critical business cycles, control objectives and key internal controls

In December 2002, Deloitte & Touche conducted an informal poll of approximately 100 financial services clients including banks, securities firms, insurers and investment managers. Participating were the professionals who are driving their firms' responses to Sections 302 and 404. We asked how well positioned they believed their firms were to comply with the internal control requirements of Sarbanes-Oxley. More than 90% of the responses fell into one of two categories: either the respondent believed that only minor changes are required, or he/she simply did not know what steps their firms needed to take. The reason for this split reflects the client's industry perspective. Banks felt that only minor changes are needed to their internal control environments because of compliance with existing regulations, while other organizations (mostly securities and insurance firms) were less clear about the implications to their governance structure.

At the center of Sarbanes-Oxley is the deep connection of financial services with the capital markets, the economy and the public's trust in our financial system. While the full impact of this legislation is still evolving, the challenges it presents require actionable responses now.

Industry Segment Challenges

The state of readiness for Sarbanes-Oxley compliance varies considerably by industry segment. Financial institutions need a clear picture of the challenges specific to their own sectors. The following discussion highlights issues that are integral to developing the action items to facilitate the compliance process in each.

Banking

In general, depository institutions -- banks and thrifts -- are the best-prepared segment of the financial services industry for Sarbanes-Oxley compliance. For more than a decade, they have been required to comply with the Federal Deposit Insurance Corporation Improvement Act of 1991 (FDICIA), after which many of the internal control requirements of Sarbanes-Oxley were modeled.

However, even for banks, additional work is likely to be needed. For example, the need for CEOs and CFOs to supervise non-financial disclosures such as certain market risk measures and their integration with internal controls, is new to Sarbanes-Oxley and is not covered by FDICIA. In addition, Sarbanes-Oxley calls for compliance at the holding company level, so subsidiaries that were exempt under FDICIA will now be examined. As a result, some banks will have to broaden and enhance their internal controls and documentation to cover a larger number of entities (e.g., asset management, broker-dealer or insurance subsidiaries).

Sarbanes-Oxley has substantially raised the standards for banking regulatory agencies about what their examiners should expect to find when evaluating the internal controls and assessment practices of the institutions they supervise. Banks whose compliance falls short of the new, broader Sarbanes-Oxley standards can expect regulatory scrutiny ahead.

One issue that has yet to play itself out is that of jurisdiction. While the banking regulators have signaled a move toward Sarbanes-Oxley and away from FDICIA, the Act itself gives the actual enforcement authority for Section 404 not to them, but to the Securities and Exchange Commission (SEC). In addition, banking institutions whose securities are also traded outside the United States may encounter rules in those countries that differ from ours.

As alluded to earlier, banks' risk management practices have undergone significant development over the last decade. While internal controls themselves have often kept up, many institutions have not yet fully integrated into their internal control assessment processes the benefits gained from this focus on risk management or the additional areas of risks now identified and self-assessed.

Many banks, especially the larger institutions, have emphasized the development of additional revenue sources from new lines of business. These business lines often now represent a substantial portion of the enterprise, but their internal controls may not be as rigorous as those in the more traditional lending and trading businesses and may not meet the high standards of the current regulatory environment.

Outsourcing, cooperative ventures and other aspects of the extended enterprise continue to play an increasing role in banking. However, many banks have outsourced critical aspects of internal control, but their assessments may not adequately take such “external internal controls” into account.

The bottom line is that banking is all about the public’s confidence. Nowhere is the need for “best practices” in internal controls and their assessment greater than in banking. In the current environment, banks and banking regulators have begun to question whether their processes, including FDICIA, are “leading edge.” Audit Committee members and other directors who sit on bank and non-bank boards are asking “best practices” questions; CEOs and CFOs need to be able to answer in a positive fashion.

Securities

In marked contrast to depository institutions, securities firms have not had to live with the requirements of FDICIA. Until the enactment of Sarbanes-Oxley, their principal oversight bodies, the SEC and self-regulatory organizations, have focused on capital adequacy and customer protection, rather than safety-and-soundness. As the SEC gears up to enforce Sarbanes-Oxley, its regulatory focus will expand.

Among the core competencies of the securities industry are the management of market and counter party risk, and efficient clearing and settlement with a minimum of "fails" and other operational errors. Large amounts of money pass through the system daily. As a consequence, the quality of securities firms' internal controls is generally high. However, until the advent of Sarbanes-Oxley, they have not been required to document their control processes as banks have, nor to perform the annual evaluations of internal controls that banks must do to satisfy the requirements of bank examiners and their independent auditors.

Moreover, the financial disclosures of banks have long been subject to detailed regulatory requirements, far more so than those applying to securities firms.

In recent years, securities firms have been impacted by significant changes to the financial reporting requirements for their structured products and securitization businesses. These changes, most significantly SFAS 140, which deals with reporting asset transfers (securitizations) and FIN 46, which addresses the identification and potential consolidation of Variable Interest Entities, have the potential for material financial statement impact. Securities firms have worked diligently to develop processes -- often outside of core transactions processing systems -- to evaluate all transactions subject to these financial reporting requirements, but

AMERITRADE

An Early Adoption Success Story

Ameritrade, based in Omaha, Nebraska and founded in 1975, is a leading provider of online brokerage services. Despite current market conditions, the firm has grown rapidly through a series of major acquisitions, including Tradecast and National Discount Brokers in 2001 and Datek in 2002. Today, its approximately 2,000 employees serve more than 2.8 million client accounts.

Several years ago, Chairman and Founder J. Joe Ricketts set out with the Board to take advantage of growth opportunities and transform Ameritrade from a younger, entrepreneurial company into a more professionally managed one. A central part of this transformation was Ameritrade's Internal Control Assessment Program, launched in late 1999. A new vice president joined the company, and drawing upon his previous banking experience, the decision was made to pattern Ameritrade's documentation and assessment of internal controls on the process that banks follow under FDICIA. A risk-based COSO framework, as developed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) and sponsored by the AICPA in 1991, was adopted at the outset.

As a result of this program, Ameritrade was able to include in its 10-K for the fiscal year ending September 29, 2001 a Report of Management, which covered internal controls. After the enactment of Sarbanes-Oxley, not only was Ameritrade well positioned to comply with Section 302, but also became an early adopter of Section 404 by asking Deloitte & Touche to provide an attestation report regarding internal controls on the Report of Management included in its 10-K for the fiscal year ended September 28, 2002.

Among the conclusions derived from Ameritrade's experience:

- Senior management buy-in is critical: up front and throughout the process
- Documentation of controls must be consistent from system to system, and from department to department
- Integration of acquisitions should begin quickly, before closing to the extent feasible
- Ameritrade's initial assessment program took nearly two years to complete. Companies no longer have the luxury of so much time.

most have not yet developed sustainable routine processes and control environments to assure consistent financial reporting. Given the potential for material financial impact, these firms will need to quickly develop and implement internal control processes.

Several of the points made in the previous section about banking also apply to the securities industry. Because Sarbanes-Oxley is concerned with the parent-company level and embraces all corporate activities, all subsidiaries, including those heretofore unregulated, will have to be brought into a generally accepted internal control framework. In addition, many securities firms have also made use of the extended enterprise by outsourcing functions and business operations. This outsourcing transfers responsibility for internal control to the outsourcing partner. Management must determine the nature and timing of internal control assurance from all major outsourcing vendors.

Those firms that operate multinationally are also likely to encounter differing, and possibly conflicting, regulatory environments. The most practical approach to dealing with these numerous governance and control requirements will ultimately be to find the common aspects of the various rules and start with a common governance and internal control philosophy.

If Section 404 becomes effective by September 2003, as is quite possible, some securities firms -- those whose fiscal years end in November -- will have even less time in which to prepare for compliance than those companies reporting on a calendar-year basis. They would thus be among the first companies in the United States to face the challenges of the requirements of Section 404.

As is the case with banking, restoring investor trust is vital to the health of the securities industry. Adopting and implementing best practices for compliance with the internal control provisions of Sarbanes-Oxley can be fundamental to achieving that goal.

Insurance

Like securities firms, the insurance industry has not been held accountable for the documentation and evaluation of internal control standards that FDICIA has required of banks. In addition, insurance companies must address issues of their own.

All financial services companies face disclosure issues involving elements of subjectivity, e.g., the valuation of inactively traded or non-traded securities. However, the unique nature of insurance risk (the quantification of which is often inherently difficult and judgmental) is leading many insurers' disclosure committees to involve claims, underwriting and actuarial personnel -- groups that traditionally have not been a core part of a financial disclosure team.

In addition, many states are currently considering the possible enactment of their own, state-level, Sarbanes-Oxley-type legislation. While such developments would affect all segments of the financial services industry and raise the possibility of having to comply with as many as 50 different sets of state rules, the impact on the insurance industry would be substantially greater because the states are the industry's primary regulators. Some proposals under consideration would extend Sarbanes-like requirements to companies that are not subject to SEC filing requirements, including mutual insurers.

While not covered by Sarbanes-Oxley, mutual insurance companies also have an interest in ensuring that their internal controls are equally as effective as those of their stockholder-owned competitors. For them, too, the integration of internal controls with top-level corporate governance, and the periodic evaluation of internal controls under a recognized control framework against industry "best practices" is important in protecting their brand and image, as well as the interests of their policyholders.

Registered products are exempt from Section 404, but mutual insurers that issue them must comply with Section 302. Typically, the operations, financial reporting and disclosure controls that support these products are commingled with those supporting other products that may not require certification. The precise scope of the certification and evaluation of disclosure controls and procedures must be defined and documented. To date, the SEC has provided no guidance on this issue.

Investment Management

Under Section 405 of Sarbanes-Oxley, investment companies (mutual funds) registered under the Investment Company Act of 1940 are exempt from the internal control assessment and auditor report requirements of Section 404. However, they are still subject to the requirements of Section 302, and asset managers that are public issuers are subject to the requirements of Section 404.

Due to the nature of the mutual fund industry, specifically the breadth of products sold by asset managers, many large mutual fund complexes will file hundreds of Section 302 certifications each year. Consequently, the CEO and CFO will need to devote a significant amount of time to the control evaluation and certification processes. Consequently, many complexes are devoting substantial resources to develop a certification process that is not only effective, but also efficient.

ALLSTATE

Concentrating on Well-Documented Internal Controls

Allstate, based in Northbrook, Illinois, is one of North America's leading financial services companies, providing insurance, banking and asset management products to more than 16 million households.

Planning for Allstate's internal controls program began in earnest in February 2003 with the identification of key people at the business-unit and corporate levels to form a Project Management Office, as well as the outside resources that would be required. Critical to the program's success, each of Allstate's five business units appointed an "owner" within its senior management, an executive with a strong commitment to the project who took personal responsibility for its progress.

The COSO framework, together with the associated CobiT framework as defined by the Control Objectives for Information and related Technology, was adopted early in the project. Documentation standards and application guidance were developed for all business units yielding a common approach consistently applied throughout the company. Allstate's timeline called for the bulk of documentation and assessment to be completed by the end of July, to allow for remediation prior to Deloitte & Touche's attestation work in the fourth quarter (Allstate reports on a calendar-year basis). By the end of March, the program was already well along.

Among the conclusions derived from Allstate's experience:

- Start early, when planning can be done most effectively
- Identify the best and most appropriate people and commit them to the project
- Try for early successes to build confidence and support throughout the organization
- Concentrate on the goal of sound, well-documented internal controls, rather than the technology
- Involve your financial audit team -- internal and external -- early in the process to reduce the possibility of "surprises"
- Build a sustainable process that is embedded into the company's business, rather than a one-time project

At smaller fund managers, resources are typically thinner. Such organizations are struggling with how to meet the requirements of Section 302 without adding personnel to the organization. Unlike larger complexes, which have a larger asset base over which to spread Sarbanes-Oxley-related expenses, additional costs of complying with Section 302 may have a significant effect on the performance of the funds. Many small funds will be challenged to allocate the people and financial resources to establish such controls without impacting their funds' performance.

The effort is further complicated by the decentralized nature of the mutual fund industry and the extensive reliance on external service providers -- such as distributors, custodians, record keepers and transfer agents. In developing an evaluation process, management must incorporate the operational and control structures of all of its key service providers -- which requires reliance upon information that it does not directly control. As a result, the mutual fund industry needs to define up front the extent and timing of assurances that each firm expects to perform.

Because mutual funds are required to close their accounting records daily and record all components at market value, the industry has built a very detailed and tightly controlled record keeping process -- a fact that is borne out by the lack of headlines surrounding mutual fund accounting errors. Subsequently, many asset managers believe that Sarbanes-Oxley provides little additional "real" comfort to mutual fund shareholders while, in many instances, increasing the expenses that are passed on to them.

How **We Can Help**

The Deloitte & Touche Solution Set

Start at the End

Start with the end result in mind -- financial services companies need a robust internal change management function, a process where any change to the control environment is recognized, evaluated and determined to be in line with senior executives' and the Board's wishes. The CEO and CFO can use this process to review the internal control environment on a regular basis.

Inventory

Conduct an inventory of existing internal control processes and information assets. For many firms, senior management will find that information already in place can be leveraged to support Sarbanes-Oxley compliance. For example:

- Documentation produced by Internal Audit as a result of the recurring audit activities may contain significant descriptions and results of testing of the internal control environment
- Policies and procedures promulgated by the controller function may specifically address internal controls related to financial reporting
- Many firms currently have high-level risk management functions such as new product committees, operational risk committees and the like that can provide the basis for an executive-level steering committee for a Sarbanes-Oxley initiative

Internal Control Assessment

Adopt and, if necessary, adapt a recognized internal control framework, such as that promulgated by the Committee of Sponsoring Organizations (COSO) through which to perform your design and assessment of internal controls. COSO is clearly the most widely accepted such framework in the United States, and is the one with which regulatory agencies are likely to be most comfortable.

Top-Down Approach

Develop a "top-down" approach to documenting and assessing internal controls. For every major business function, it is likely that there is a sub-set of critical controls relied upon by management to ensure that transactions are accurate, complete and properly recorded. To identify these critical controls, begin with the corporate financial statements. Identify the major business cycles related to every line item that meets any of the following Sarbanes-Oxley criteria:

- Material to the financial statements themselves
- Critical to achievement of major goals and objectives of the business
- Relates specifically to compliance or disclosure
- Critical to achievement of financial control assertions

For each business cycle, identify the potential risks involved (e.g., completeness, accuracy, authorization) and the specific internal controls that are critical to managing those risks. Use these critical controls as the initial baseline for future changes and maintenance.

Using technology that is either purchased or developed as a customized solution, build an automated controls repository to document control objectives and activities, map activities to control objectives and identify deficiencies on an ongoing basis. Develop and perform the initial and ongoing tests on which management's assertion and control reporting will be based.

Address Known Weaknesses

Start sub-projects to address internal control weaknesses as they are identified. Many organizations have internal control areas with which they struggle. Among those we have encountered frequently are:

- Updating systems with new or required features
- Reviewing areas that require judgments by management or significant manual processing
- Managing third-party vendors

If Internal Audit has had recurring recommendations in specific areas, deploy resources to have credible responses to these identified weaknesses before Section 404 implementation is required.

The Sarbanes-Oxley Clock Is Ticking

As noted at the outset, Section 404 is likely to become effective as early as September 2003. For many financial services firms, especially those which are large and complex, preparations for internal controls compliance will have to be well along during the spring and summer months in order to have in place the basis for the assertions and attestation that must be complete by the fall.

While many financial services firms already have strong internal control structures in place, the new requirements will clearly impose challenges. The key to success will be to leverage and extend internal control resources and incorporate the changes into existing change-management functions.

A Call to Action

Deloitte & Touche is ready to help you navigate the complexities of Sarbanes-Oxley and gain the benefit of improved governance, controls and financial reporting. The professionals of our Financial Services Industry practice have the depth of experience to help clients establish control processes and reporting tools that can advance compliance throughout your organization.

Contacts

Subject-Matter Specialists
Henry Ristuccia
hristuccia@deloitte.com
212-436-4244

Doug Finn
dfinn@deloitte.com
212-436-4441

Industry Contacts
Carol Larson, Banking
clarson@deloitte.com
412-338-7210

Dawn Patterson, Securities
dapatterson@deloitte.com
212-436-6861

Paul Kirwan, Investment Management
pkirwan@deloitte.com
617-437-2477

Gary Shaw, Insurance
gashaw@deloitte.com
973-683-7025

About Deloitte & Touche

Deloitte & Touche is the U.S. member firm of Deloitte Touche Tohmatsu, one of the world's leading professional services organizations. DTT member firms deliver world class assurance and advisory, tax and consulting services. Their more than 95,000 people in 140 countries serve over one quarter of the world's largest companies, as well as large national enterprises, public institutions, and successful, fast growing global growth companies.

Our internationally experienced professionals strive to deliver seamless, consistent services wherever our clients operate. Our mission is to help our clients and our people excel.

Deloitte Touche Tohmatsu is a Swiss Verein, and each of its national practices is a separate and independent legal entity.

Deloitte Touche Tohmatsu member firms serve financial services firms globally through our global financial services industry practice. GFSI's industry specialists represent every major financial center in the world and bring decades of experience and leadership in banking, securities, insurance and investment management to each client assignment. For more information about our practice visit our web site at www.deloitte.com/gfsi.

04/03 – #3092

Deloitte
Touche
Tohmatsu