RECORD Volume 30, No. 2*

Spring Meeting, San Antonio, TX
June 14–15, 2004

Session 33OF
Sarbanes-Oxley Compliance: Ready or Not, Here It Comes

Track: Financial Reporting

Moderator: DARIN G. ZIMMERMAN

Panelists: BRAD IRICK†
JAMES A. MILES
RAYMOND SMITH††

Summary: This session addresses aspects of the Sarbanes-Oxley Act, including a discussion of the history and purpose of the act, processes of compliance and their documentation, identification of key controls and testing for key control effectiveness.

MR. DARIN G. ZIMMERMAN: I am with the corporate actuarial department of AEGON in Cedar Rapids, Iowa. As I was preparing my introduction and my opening remarks, I was thinking that sometimes you come to these SOA sessions, and you walk out thinking it was fascinating. Sometimes you attend, and you walk away thinking that is something you can use and that is going to make you 100 percent more productive. It is going to make you more profitable. It is going to make you more efficient. I don't think that's going to happen today.

Of course, sometimes the topics are timely. In today's *Wall Street Journal*, there is an editorial, written by Paul Volcker and Arthur Levitt, entitled, "In Defense of Sarbanes-Oxley." The one-sentence summary is they believe the benefits of the legislation outweigh the costs. Last week there was a similar editorial written by John Thain, who's the CEO of the New York Stock Exchange. He wrote an opinion contrary to this saying that it needed to be reviewed.

---

†Brad Irick, not a member of the sponsoring organizations, is partner at PricewaterhouseCoopers LLP in Houston, Texas.

††Ray Smith, not a member of the sponsoring organizations, is partner at Ernst & Young LLP in Des Moines, Iowa.

At the very least, this is a timely subject. I know many of your companies need to comply with it for 2004, and the foreign filers get a little extra reprieve. The three speakers that we have today are going to do everything in their power to try to convince you it's a fascinating subject. Immediately to my left is Jim Miles. Jim is an FSA. He is a senior manager with Deloitte Consulting in Indianapolis, and he has 25 years of experience with financial reporting. He is also currently the general chairperson of the SOA's Education and Examination Committee.

Next to Jim is Ray Smith. Ray is a CPA. He is a partner with Ernst & Young in Des Moines, Iowa. He has had 31 years of insurance company audit experience and lately he's devoted a lot of his time to 404 advisory.

At the end of the table is Brad Irick. Brad is also a CPA. He is an audit partner with PWC in Houston, and he has 15 years of varied experience with life and property and casualty companies. He has mainly performed audits. With that, I would like to call up Jim.

MR. JAMES MILES: On November 8, 2001, the Enron Corporation announced that its earnings were overstated by $800 million. Less than one month later Enron filed for bankruptcy. The Standard & Poor's (S&P) 500 ended that year at 1,149. Three months later, in March '02, the accounting firm of Arthur Andersen was charged with obstruction of justice by the U.S. Justice Department for destroying documents related to Enron.

The weeping and gnashing caused by these and other accounting and auditing issues caught the attention of the 107th Congress of the United States. The Financial Services Committee of the House of Representatives, chaired by Republican Michael G. Oxley of Ohio, deliberated a bill to address the perceived problems. The committees received numerous reports and inputs from accounting and other industry lobbyists. On April 24, 2002, the U.S. House of Representatives passed the bill it was working on. Meanwhile, over in the Senate, Senator Phil Gramm was leading Republican members of the Senate Banking Committee in opposition to the bill that was being deliberated there. The Senate Banking Committee is chaired by Senator Paul Sarbanes, a Democrat from Maryland. By mid-June '02, most observers considered the bill dead and unlikely to pass.

On June 26, 2002, WorldCom Corporation announced accounting irregularities of $3.8 billion related to the recognition of certain expenses. The confluence of another company's announcement of a major accounting irregularity in a declining stock market broke the dam of opposition. The Senate Banking Committee passed a bill, and it was sent to the Senate floor where it passed on July 15. The House and Senate bills were sent to a conference committee on July 25, and, with one dissenting vote, the bill passed the conference committee.

Senator Phil Gramm of Texas cast that lone dissenting vote. In recognition of the location of this meeting, and to underscore the atmosphere surrounding the

passage of the act, I'd like to present the following quote by former Senator Phil Gramm: "I want to make it clear that this bill could have been a lot worse. In the environment we're in virtually anything could have passed Congress." Senator Gramm could just as easily have said, "Sarbanes-Oxley compliance: Ready or not, here it comes."

Thirty-four days after WorldCom announced its $3.8 billion accounting irregularity, President George W. Bush signed the Public Company Accounting Reform and Investor Protection Act, commonly known by its short title, the Sarbanes-Oxley Act of 2002. The S&P 500 closed that day at 903, 19 percent below the level it held on the day that Enron announced its $800 million problem just nine months earlier. The passage of the Sarbanes-Oxley Act of 2002 impacted 15,000 U.S. public companies and their auditors.

We're going to spend a few minutes looking at important terms and concepts, and then we'll get to Brad and Ray, who'll talk about the stuff you really want to know, and that's the specific implementation issues for companies and their auditors.

The Sarbanes-Oxley Act of 2002 required the U.S. Securities and Exchange Commission (SEC) to promulgate rules to implement the act. In his testimony before the Senate Banking Committee in September '03, William H. Donaldson, chairperson of the SEC, stated the commission had undertaken 15 separate rulemaking projects to implement many of the provisions of the Sarbanes-Oxley Act, many of them with short deadlines.

Under the House version of the bill, private groups would have been allowed to set up oversight boards that would have operated with the approval of the SEC. Opponents were concerned that the resulting boards would be controlled by the accounting profession. Senator Sarbanes refused to back off the provision in the Senate bill that established an oversight board. Title I of the Sarbanes-Oxley Act of 2002 established the Public Company Accounting Oversight Board (PCAOB), and the board was given three specific purposes: to oversee the audits of public companies; to protect the interest of investors; and to further the public interest in the preparation of informative, fair and independent audit reports.

The Sarbanes-Oxley Act of 2002 included restrictions on the membership of the Board. As in most legislation, the membership requirements resulted from compromise. The members must serve on the board full time and cannot engage in any other professional activities. The members must be financially literate. The members are appointed by the SEC in consultation with the secretary of the Treasury and the chairperson of the Board of Governors of the Federal Reserve System. The board's '04 fiscal year budget of $103 million gives some measure of the enormity of the task the board faces. The revenues for the board principally are derived from assets collected from public companies.

At this point you're probably wondering what financially literate people look like.

Let's take a minute to meet the members of the board. William McDonough is the current chairperson. He's a former president of the Federal Reserve Bank of New York. Kayla Gillan is a former general counsel to the California Public Employees' Retirement System. Daniel Goelzer is a CPA, a former partner in a law firm and a former SEC general counsel. Bill Gradison is a former U.S. congressman. Some of you may remember Mr. Gradison is a former president of the Health Insurance Association of America. Charles Niemeier is a former chief accountant in the Division of Enforcement of the SEC, and he's also a former CPA. As you can see, the board members are, as Section 101 of Sarbanes-Oxley Act requires, prominent individuals of integrity and reputation. The PCAOB has been given a great deal of authority, but it is important to remember that its actions are subject to the scrutiny and oversight of the SEC.

The Sarbanes-Oxley Act of 2002 has 69 sections. We've already talked about a few of them in relation to the formation of the PCAOB. However, some sections are so prominent that they've achieved the ultimate section status and can now be referred to by their number only. We are going to highlight two of those sections today, 302 and 404.

Section 302, corporate responsibility for financial reports, requires rules to be promulgated within 30 days of the passage of Sarbanes-Oxley. The section requires that the principal executive officer and the principal financial officer make certain certifications about the financials of their company.

Section 404, management assessment of internal controls, requires rules to be promulgated that require each company's annual report to contain an internal control report. The internal control report must first state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting and second must contain an assessment of the effectiveness of the internal controls and procedures for financial reporting. The section also requires the auditor of the company to attest to and report on the company's assessment of its internal controls.

Section 103 of the Sarbanes-Oxley Act requires the PCAOB to establish auditing, quality control and independent standards in order to implement the requirements of Sarbanes-Oxley Act of 2002, such as those in Section 404. In April '03, the PCAOB accepted the preexisting professional standards as the board's interim standards. The board subsequently determined that the existing standards governing an auditor's attest of internal controls were insufficient for Section 404, and on October 7, 2003, the board proposed the auditing standard, an audit of internal control over financial reporting in conjunction with an audit of financial statements. On March 9, 2004, the board approved PCAOB Accounting Standard No. 2.

Three important terms are defined in the standard: control deficiency, significant deficiency and material weakness. A control deficiency can be a deficiency in design

or a deficiency in operation. A deficiency in design means that the control is missing or that a control exists and operates as designed, but it doesn't always meet the control objectives. A deficiency in operation means that a control does not operate as designed, or the person performing the control does not have the necessary authority or qualifications for that control.

A misstatement on the company's financial statement that will not be prevented or detected is a serious risk. Significant deficiency and material weakness are used to classify that risk. The key phrases for identifying a significant deficiency are: "more than a remote likelihood" and "more than inconsequential." If you look at it closely, you'll see those words stand out. The key phrases for identifying a material weakness are "more than a remote likelihood," which is the same as significant deficiency, but the second key word is "material misstatement." "Remote likelihood" is defined in Financial Accounting Standard (FAS) 5, Paragraph 3.

In order to implement internal controls, you have to have a standard. In 1985, the Committee of Sponsoring Organizations (COSO) created the National Commission on Fraudulent Financial Reporting. I want to emphasize '85. It created the commission to identify causal factors of fraudulent financial reporting and to make recommendations to reduce its incidence. The commission is commonly known as the Treadway Commission after its chairperson, James C. Treadway.

The commission's report issued in '87 made several recommendations that address internal controls, and a task force was formed to review literature on internal controls. The task force in turn recommended that COSO undertake a project to provide practical broadly accepted criteria for establishing internal controls and evaluating their effectiveness. The resulting study and report were released in '91, entitled "Internal Control Integrated Framework." The report was and is the generally accepted internal control standard in the United States. The Sarbanes-Oxley Act and/or the PCAOB does not require that the COSO report be used, but there aren't any other alternatives.

According to the report, there are five components of internal control. Control environment is the tone of the organization, or the "tone at the top," which was a phrase coined there. Risk assessment is identifying the risk and analyzing the likelihood and impact of that risk. Control activities set policies and procedure that assure that management's directives are carried out. Information and communication is capturing and communicating relevant information. Monitoring ensures that the systems are performing as intended.

When the Sarbanes-Oxley Act of 2002 passed, there was immediate concern that each state, acting to protect the investors in its state, would promulgate legislation similar to Sarbanes-Oxley Act of 2002, and the result would be an unsolvable maze of regulations. The American Institute of CPAs worked through its state chapters to mitigate the likelihood of the so-called cascade effect. The white paper, "A Reasoned Approach to Reform," was distributed to provide support for this effort,

and you can find a copy of that paper at the American Institute of Certified Public Accountants (AICPA) Web site at *www.aicpa.org*. The National Association of Insurance Commissioners (NAIC) established a working group to develop a model regulation that paralleled the Sarbanes-Oxley Act of 2002.

It is likely that insurance companies not currently impacted by the Sarbanes-Oxley Act of 2002 will eventually be subject to many of the same rules. Some are arguing that insurance companies already have more reporting requirements and heavier capital requirements than other industries and that additional regulation is unnecessary. However, the chairperson of the working group believes that the benefits will outweigh the cost. The working group has stated that it will not get ahead of the process that's currently in place for implementing Sarbanes-Oxley, but it anticipate that the model regulation will have an effective date of '06.

There are a lot of good resources available on the Internet. If you go to the NAIC Web site at *www.naic.org*, you can review the latest draft of its model regulation.

Audit firms have also made significant investments in ramping-up to deal with Sarbanes-Oxley. Your auditor can be a big help in sorting out what your company needs to do to comply with the Sarbanes-Oxley Act of 2002, because, ready or not, here it comes.

MR. RAYMOND SMITH: With that as a background, I'm going to focus on one of the elements there—Section 404. Again, this is the piece dealing with internal control over financial reporting. As we get into looking at the definition of internal control, it's going to be even smaller than some of the other definitions of internal control that include operations and compliance matters.

I'm going to try to cover how companies are implementing Section 404. Going back to Jim's comments, management is having to attest that it has effective controls over financial reporting, and then the auditors come in behind and have to issue an opinion. In fact, it will be a couple of opinions on internal control and an opinion on financial statements integrated going forward. I am the management guy, and Brad will come in behind me and be the auditor. He'll clean up whatever it is that I have to say here. Again, I'm going to talk about a methodology for doing this, and it's one of many methodologies. It's just one that I am familiar with.

I'll share some best practices and lessons learned from having done this. As I think Darin pointed out, I've done this from both perspectives—being an advisor and also an auditor. You can't do the same for both companies. You have to be careful under the independence rules. My firm has also done quite a bit of surveying. As I go through this, I'll try to give you a flavor for where companies are and what some of their experiences have been. Hopefully there's something here for those accelerated public filers that are having to report as of December 31, 2004. I guess you have probably some view of what completion looks like.

The foreign filers that Darin mentioned and those that aren't accelerated public companies have until December 31, 2005, although I suspect they're in the middle, as we speak, of at least the documentation phase, and then ultimately others probably are waiting to see, as Jim mentioned, where the NAIC is headed with all this. We're not going to be able to cover a lot in 20 minutes, but at the end of 20 minutes I want you to have a couple of things in mind. Understand that this is a big deal if you're ever saddled with it. It's not like a Y2K type of a project. It's a big deal involving a significant investment of resources. It's also a cultural change, so it's something that you're going to have to live with not only this year but in the years to come.

Starting at 30,000 feet, how do the rules define what management's requirements are? I think Jim mentioned this PCAOB that has issued, although the SEC I think has yet to approve, a standard that defines management's responsibilities. What does management have to do with internal control reporting over financial reporting? Certainly management will have to accept responsibility for the effectiveness of internal controls. This is not something that you're going to be able to lay off on your auditor. I think Jim mentioned management will have to evaluate the effectiveness of internal controls using suitable criteria. He mentioned COSO. I'm not aware of any other one that's out there, but certainly COSO has a target that we all have to shoot for.

Management has to support its evaluation with sufficient evidence and documentation. Again, the standard calls for a fairly rigorous process, and we'll walk through that in a second. It differs from the 302, the management certifications that have been going on in public companies and that even have to do with regulatory filings. The standard there is probably, to the best of my knowledge, when people sign that the financial information is accurate, and they have controls in place. Section 404 now requires companies to accumulate positive evidence supporting their assertions that they have effective internal controls, so it's different from the certifications that people have been signing. Public companies will have to report, and that's part of the NAIC proposal as well, but they will also have to provide a written assessment as of the end of the year that they have effective internal controls.

Even further, there is this positive evidence. You have to accumulate sufficient documentation. In fact, not having documentation out there is mentioned in the standard as a weakness in and of itself. You can get yourself into a reporting situation by having inadequate documentation. This means not only documentation stating that you've documented processes, what-can-go-wrongs and controls, but even if you have a control there, somebody's doing his job, but you're not documenting the signoffs. The controls have to be testable and be able to be monitored. That's particularly true in a lot of the actuarial areas where we know there are reviews going on. We know there are controls out there. Now you have to go that extra mile and sign off and save your e-mails to prove evidence that those controls are working, and I'm sure Brad will get into some of that when he works

through it.

Some of the 404 requirements can have some business implications. The scope has to include entities acquired on or before the end of the year. Your assessment is as of a point in time, as of the end of the year, so you have to include companies that you acquire. You have to build this into your due diligence process. Companies may even shy away from doing acquisitions in the fourth quarter.

There are other things that have business implications as well. Think about IT conversions. Does it make sense to have a lot of IT conversions in the fourth quarter if now all of a sudden you have to turn around and assert that you have effective controls? You have to have some period of time before that last day of the year to be able to demonstrate that controls over that new system are functioning. It may cause delays, but it could cause you additional cost in running parallel for longer periods of time.

It also gets into a lot of reinsurance. The perspective of these rules is gross rather than net relative to ceded reinsurance. In fact there are companies that thought they got books of business off their books, never to have to worry about them again through reinsurance transactions but that now have to be concerned with how the assuming company is accounting for things that are on their books net zero but in their financial statements in various places on a gross basis. The point is this could have some business implications.

How are companies implementing this? Chart 1 shows what an end-to-end 404 project plan might look like. From management's perspective, left to right, there's a planning phase and also an execution phase. Planning and scoping the project are on the left. This list of activities is important. In fact there is a lot of additional cost, a lot of rework and a lot of frustrations in companies not spending the necessary time up front doing these planning and scoping activities. This includes determining what your significant accounts are and mapping your significant processes and business units to the financial statements to those significant accounts.

Proceeding to the right, there are additional activities in the execution phase. These include documenting significant processes and controls (I'll define those in a second), then turning around and evaluating the effectiveness of the controls, testing the significant controls that you identify, and, finally, identifying issues for remediation. Back to the theme, this is not a one-time deal. You have to set monitoring systems in place after you do it initially to be able to do this almost on a quarterly basis to support some of the financial filings that you do. You ultimately end up with management's report to the public, its assertion that it has effective internal controls. Then auditors come in behind and report on that management assertion, and they also have to do enough procedures to issue an opinion on control effectiveness.

Today, for those companies with December 31, 2004 deadlines, about 34 percent of

the companies are still in the documentation phase. Sixty-four percent have now proceeded from the documentation phase and are doing evaluation and testing. We've estimated that only about 2 percent of the companies are in a position today to be doing their public reporting. Companies are in various stages, and it doesn't vary a lot. Certainly they'd be a little bit farther behind for those companies with the December 31, 2005 deadlines.

A few companies are also projecting that they'll be finished in the last two months of the year before they have to actually report on 404. A key thing is that you'll want to get started and get finished as early as possible prior to the end of the year. The reason for that is that maybe you have some controls that aren't working. You have some documentation that doesn't exist. It allows you to get remediated controls and procedures in place so that you can demonstrate that they're operating for a sufficient period of time for the auditor that comes in on December 31 and has to report on those controls. Allow yourself time for remediation.

That's what a project plan might look like. I'm going to take each of those and quickly walk through some of the details. What's our target? What's internal control all about? Chart 2 is the COSO cube that Jim referred to. It is defining internal control as regulatory compliance, operations and financial reporting. So 404 deals with controls over financial reporting, although most companies are expanding that a little bit to cover a couple of the control components that Jim also walked through, certainly the control environment and risk assessment. In order for the financial reporting controls to operate, you have to have strong overriding controls, a strong tone at the top. Companies are taking this is a little bit beyond what Sarbanes-Oxley requires.

In planning and organizing a project, here are some things to think about. A key to success of projects of this nature is ensuring the right sponsorship, and this has to be sponsored at the top levels of the organization. One step is identifying an appropriate project manager, somebody who can reach into the organization and get things done. This is a big project. A lot of companies are also using a 404 advisor, somebody other than the auditor, to share knowledge but also be some additional arms and legs. Each of you in this room has a job of your own. Just think of piling this on top of what your day-to-day duties are. I'm sure you're going to get asked to be participants in this. There are additional arms and legs that most companies are using. Another key to success is the company management must take ownership of this whole process.

There is a key insight that companies have woefully underestimated the time, effort and cost of doing this. In fact, companies that are now finishing probably missed their initial estimates of cost and level of effort by 25 percent to 50 percent or more. Here's some more from the surveying we've done: companies with $1 billion in revenue are spending upwards of 8,000 hours doing this. Companies with more than $20 billion of revenues are spending more than 80,000 hours. Depending on

how dispersed the company is, there are companies that are spending 100,000 hours just complying with Section 404. We truly don't know the true cost of all this because a lot of companies are in the midst of their remediation efforts right now, trying to fix some of the issues that are out there. It's a costly venture.

I'm going to walk through what a project might look like and how some of the roles and responsibilities might be dispersed. There's some limitation, I think, and audit committees certainly have not wanted the external auditors to be involved in the documentation process, but the key point is for management to own it.

Here are some high-level steps to developing a project plan and scoping the project. A lot of companies are using supporting tools and techniques and putting a repository out there for the documentation, putting in issue management. A lot of the software that's available today has some issue management and project management capabilities to it. This has to be kept current. You have to figure out a way to keep this current, to review it and to report it after your initial year on a quarterly basis.

Many times we're not starting from scratch with the companies that we walk into. One of the initial steps you do is try to figure out what the inventory of existing documentation that's out there is, whether it's internal audit or new systems that went in place that have supporting project documentation. Over the years there have been a number of process improvement efforts in companies. But look for places like that where there might already be some existing documentation that you can leverage. We're documenting controls as well as the process, but we're particularly focused on controls. As always, for anything of this size, project management skills come in handy as well.

Jumping into the documentation and evaluation phases of a 404 project, one of the requirements is that internal controls over financial reporting must be evaluated at both the entity and a significant account level. Entity-level controls are what essentially the tone at the top is. Process, transaction or application level controls are the details, the heart of the matter. At the end of the day, 25 percent to 40 percent of the assurances for a company are going to be coming out of the entity-level bucket, and 60 percent to 75 percent of the assurances, however you measure materiality, will be coming out of the bottom bucket. It's rolling up your sleeves and getting into the details.

There are other areas in addition to documenting processes and controls. We also have to look at things like segregation of duties, safeguarding of assets and direct special attention to the financial statement close process, and all of these are embedded right in the standard.

Chart 3 shows the heart of the work, an end-to-end view of getting in and having to document at the transaction and process level. This moves from left to right. Everything trails, and, again, this is just one methodology. There are other ways of

doing this, but essentially you're starting with your financial statements as well as all the disclosures in financial statements. Materiality is a factor and a consideration in evaluating financial statements. It is a factor in how you go about documenting internal controls.

There's a small list on the top third of the page of how you go about identifying or translating those financial statements into your significant accounts, and then what your assertions, existence, occurrence, completeness, valuation, measurement, rights and obligations are. What are all the assertions around each of those significant accounts that get into your financials? You have to map back to what the significant processes are that drive balances and entries into all the accounts that ultimately end up in your financial statements. You do that mapping and take an inventory of all of your routine, nonroutine, estimation and IT processes.

For each of those, the next step would be trying to figure out what your risks are, trying to figure out for each of those assertions and accounts what can go wrong and documenting that. There's an example at the bottom. What do you have for what can go wrong? That's where your controls arise. You try to identify the proper mix of prevent and detect controls that you have in place to take care of those what-can-go-wrongs that map back to processes that map back to the financial statements.

Are you getting a feeling for this as a fairly detailed process? Actuarial would touch on a lot of the nonroutine and estimation processes, which are the more difficult areas, the areas for which the auditors have typically not relied on controls in the past. But those controls also then get tested. You have to monitor them because you're going to have to demonstrate ongoing effectiveness, with the ultimate goal being to report to the public.

I'd like to go back to this survey we talked about. Sixty-seven percent of companies have 25 or fewer processes per location, but there are many others that have 50 processes, double that for subprocesses if you can think of all your product lines per location. That's going to then get into thousands and thousands of controls that you have to sort through, although about 50 percent of those controls you'll end up ultimately testing. I'm trying to give you some idea that this methodology, this project, is fairly sizable.

For XYZ Insurance Company, a typical insurance company, here are the types of significant accounts that you would run into. Deferred acquisition cost (DAC) and value of business acquired (VOBA), benefit reserves, unearned premiums and claim reserves would all be things that the actuaries would be involved with. What are some of the processes that those significant accounts would then map to? I have also gone in and picked one of these as far as trying to answer the question "Where might actuaries be involved?" and taken benefit claims, claim reserves and related expense accounts and put in a mapping for a financial statement assertion. I go through all of those for the benefit and claim reserve significant account, but what

are some of the what-can-go-wrong questions, some of the risks that you need to be digging into? What are typical controls that you might find? These are all normative types of things that you would have to customize for your specific circumstances, but we're looking for a mix of prevent and detect control.

We've walked through the project and documentation steps. What are some of the key lessons learned? You can't determine your resource needs until you go through the process of mapping and do a good job of planning. Planning in this situation is good. It will pay dividends down the road. You can do a pilot project, but start somewhere. Have people review it. Having your external auditors review a pilot in certain locations will pay dividends. Particular attention has to be paid to computer controls and application controls that you build into your business process documentation, but then there are also computer-pervasive IT general controls that will require documentation almost as separate processes.

For a lot of companies, many successful projects involve working through a project management office. We're looking for all the business units in our organization to be doing things consistently as far as some of the challenges that you'll typically run into. The most common structure has control over the project centralized within a PMO:

•Provides a consistent view of the significant accounts, processes and locations to maximize approach efficiency.
•Supports decentralized approach as to business unit responsibility for documentation.
•Establishes the parameters for testing and evaluation, which generally is done by project team members, often qualified auditors assigned to each region or country.
•Allows for better management and assessment of pilot exercises during the planning stage.

I want to talk some more on the level of effort that's required and lessons learned. This is not just insurance companies. To justify cost, a lot of companies, if you're spending thousands and thousands of hours, are trying to extract some value from the process. I think right now most companies are focused on getting the compliance aspects and the documentation done. With that said, later a lot of companies are planning to go back through that documentation and challenge it from a process improvement standpoint. I think large, well-run organizations that have always emphasized effective controls have less to fear but probably also less to learn about their organizations. They're building confidence that already exists. Smaller companies, though, I think are putting together internal controls perhaps in areas where they didn't previously have controls. They're more likely to benefit and are making the real improvements in their financial reporting processes.

The key to the project is getting the right level of skills together. Here's what a project team might look like (Chart 4). The role of the actuary oftentimes is teamed up with a control specialist, actually being the content specialist in a lot of the non-

routine and estimation processes that affect the actuarial areas. You need process owners and managers to be involved who know the end-to-end process in an organization; otherwise you're going to waste your time.

I mentioned earlier that you're going to have to update this on a quarterly basis. Chart 5 gives names of some of the technology and repositories that are out there. This is an area where companies are spending a lot of time and effort, becoming frustrated because the technologies continue to emerge.

One of the biggest challenges in all this is the areas of service organizations. You think of third-party administrators (TPAs), managing general agents (MGAs) and reinsurance companies. A lot of organizations payroll IT. Actually the processes in a company reside with some other service organizations. Because they impact your financial reporting, you still have to consider those outside service organizations. You have to document and test controls as if they were part of your in-house processes, or you can get what's called a satisfactory Type II SAS 70 report. That's where a single auditor goes into a service organization and provides a control report that the various user groups use. That is one of the steps that are permitted as a way to satisfy the 404 requirements. Or you can essentially focus on the detailed controls within your own organization. You can't forget about those service organizations that are doing processes and work for you.

Here are what I think are the keys to project success. I can't emphasize enough senior management support. Early identification and remediation of control and testing issues are important. Identify them early so you can fix them and make sure that they're operating effectively. It's not uncommon for companies to identify 70 to 80 control issues that they have to deal with. A predominant number of those are in the IT area, but keep in mind that they're fairly pervasive controls. You probably have lined up a bunch of controls that are functioning but are also dependent on reports and other things that come out of IT. If the IT general controls aren't working, that may render a lot of the other controls moot.

You have to deal with IT controls. Talking about IT controls (Brad will get into this a little bit), in the actuarial area there are a lot of questions and a lot of focus on the issues of spreadsheets, having to put the same types of computer controls around those distributed systems. This concerns spreadsheets that you have in all your departments that generate accounting entries that get into financial statements. Controls have to be there, particularly a lot of the security and change management types of controls that you would run into in any distributed system.

Finally, I'd like to focus on trouble spots. What are the common trouble spots that you run into? I particularly mentioned IT, but now is the time to be thinking about the postimplementation period—Sarbanes, plus one year, let's say. This is not a one-time event, and the level of effort and the cost that companies are incurring or are about to incur in the second year and beyond has been estimated at 50 percent to 75 percent of what the year-one costs are. This will continue to be a significant

effort. Brad's going to come in now and essentially audit that. Brad will be covering the external auditor perspective.

MR. BRAD IRICK: The only thing I would add to Darin's comments earlier about why you would like to attend this session is that you might learn something to keep yourself or somebody you know out of jail. The 404, as some of you may have seen, has some stiff repercussions for noncompliance, and they involve an orange suit. That's another good reason to know what's going on here.

Ray had somewhat of an impossible task, and I probably have an equally impossible one, which is to spend 20 minutes talking about what last week I spent five days with a roomful of partners and managers in our firm talking about. How do you do an audit under 404? Of all the firms represented here, all four of the big four firms are going through an extensive process to try to get some guidelines out to people and some common understanding of the goals of this. I can tell you that it's not easy stuff. For most partners, they have probably never issued an opinion in the controls in their career, and that's one of the things that's new to an auditor on this.

Ray spent a lot of time talking about management's requirement. In the past, there were no specific management requirements and no documentation responsibilities. Now we have those. The other thing about the act, as you can probably see from the standard and discussion about management's responsibility, is that the depth and breadth of the requirement is massive and to some degree still being defined as we speak. Probably the biggest issue for an external auditor is now we have to issue an opinion. Many times clients will say, "You guys have been doing these things for years. You've been auditing controls." You say, "That's not exactly right."

In the conduct of an audit, we've always considered internal controls in determining the nature, extent and timing of our audit procedures. In many cases some people have issued these, but in limited cases we have issued an opinion on controls, and that basically needs a lot of defining around what that means and also brings liability to the auditor. It brings liability to management, as we just talked about as far as management's responsibilities. It brings liability to the auditors. It's a different game and a different way of looking at things. As you're working with your management, as you're talking to your auditors, realize it's an evolving process and one that's going to be a challenge for all of us as we make it through this next year.

I'm going to try to talk about a few of the responsibilities and challenges that I see from my side. As you'll see, the common theme on this will be it's probably your problem first as management, for those of you who will be participating, and then it becomes the auditor's problem to evaluate what management's conclusions have been and then determine what our positions are.

I'm going to talk a little bit about the standard, but we've covered that to a large degree. Management's responsibilities have been talked about. I'll address what the

auditor's responsibilities are. Then hopefully I'll have some things that you will be interested in regarding significant audit issues as we see them and some particular areas of concern.

The only thing I'll add to what's already been said about the standard is my understanding is that we expect the SEC to approve that maybe as early as this week. That will be along the process of clarification. I think we expect the standard to be approved by the SEC, but that is a step that has to happen to make everything a little clearer.

As we've talked about, the standard reinforces the concept. It's an integrated audit. You can't do a financial statement audit and not do the internal control and vice versa. It's all one audit. The course I taught was called "The Integrated Audit," and that's the way we'll be looking at it for public companies. It recognizes it's not a one-size-fits-all proposition, and different-sized companies may have different answers to some questions. We've talked about the outlining of management's responsibilities in the standard, and we'll talk a little bit more about auditors' responsibilities.

The criteria for evaluating deficiencies are going to be new for auditors and especially for management. When I say evaluating deficiencies, it's management's problem first. How are you going to evaluate the deficiencies you find along the way? We're going to ask, "What do we think about that?" Within PWC, we have a template that is going to summarize the deficiencies that are found, and management's going to need to have a similar tool. In the past in a financial statement audit, for those of you who have worked with auditors in that regard, we've had something that we call a summary of unadjusted differences, which is basically a score sheet areas where we came up with different answers than management did. We aggregate all those, and we evaluate what they mean. Are all these things material to the financial statements?

We're going to have to do a similar type of process for controls. For me (maybe it's because that's what I've done my entire career), a summary of unadjusted differences is a little easier intuitively to evaluate than a summary of aggregated deficiencies. We're all going to struggle with exactly how to do these things. A significant deficiency is a single instance of a significant item or an aggregation of other control deficiencies. How many control deficiencies equal a significant deficiency? I don't know the answer to that question. It's going to depend on the facts and circumstances you have.

How many significant deficiencies add up to a material weakness? Again, I'm not sure. I can tell you today that there's going to be a number on that. It can be one, two or more, but we're going to have to get down in the details and understand what the significance of the deficiencies are, what they're about and make some determinations about how they aggregate. Also in the standard it does have an additional requirement with regard to the 302 certification, the quarterly

certification that we're not talking a lot about today, basically updating beginning with the first quarter of '05. In essence this will be updating our process to have some additional inquiries about things that have changed. I won't go too much into that today.

There are a few reminders from the PCAOB about auditor independence. According to our points earlier, management is responsible for this process. The auditor can't be responsible for it. Here are some key points in the standard. As alluded to earlier, there are going to be two opinions that we'll issue. In most cases we'll issue three opinions, and they'll probably all be in one report. From a controls perspective, we'll issue two opinions. One is on management's assessment process. We have to evaluate as auditors whether or not management did a thorough enough process to support its assertion and assessment of the effectiveness of controls. Then we'll report on the operating effectiveness. We'll say a little bit more about that in a few minutes, and hopefully that will bring the significance of that to light.

The standard requires us now to evaluate the audit committee and whether or not it's being effective in its responsibilities. The auditor responsibilities also include talking about the use of the work of others and including service organizations. We just talked about management doing testing, maybe using internal audit to do some of that testing. You may be using external advisors to do some of that testing. How can we, as your external auditors, use that work? There's guidance in the standard about that, which is another hotly debated topic.

How can we get comfortable with controls at a third-party service provider for the company? Management is still responsible for the controls at a third-party service provider, but how can you get your hands around those? Do I need to go out to that location and do controls testing out there? Can I rely on SAS 70 reports? What are the options? A Type II SAS 70 report is a report where the auditors have gone in and tested operating effectiveness of controls at locations. This is another hotly debated topic about how management can rely on those. Can we, as auditors, share in that reliance on those SAS 70s and other types of procedures?

Another difficult question concerns multiple business units and locations. How do I decide where I need to be and what I need to document first from management, then as the auditor? Another interesting fact is that material weakness is equal to an adverse opinion. You'll only have to get to one material weakness to get to an adverse opinion, and that's a big thought in a couple of words right there. I think that scares a lot of people when they see it. If you have one material weakness, then you're not done. You have to keep going and find out if there are any other material weaknesses, but it's an adverse opinion de facto.

We said a minute ago that the big part of the standard is that you have to relate significant accounts (auditor judgment determination about what is a significant account) to relevant financial services like valuation, completeness, existence,

presentation and disclosure. The standard defines the assertions. As auditors I think we have typically thought in terms of assertions. Depending on the management you're dealing with, it may or may not have worked in thinking about assertions, but the standard requires that.

The standard requires the auditors to do walk-throughs of processes as part of their evaluation of design effectiveness. In significant locations and in significant processes and major classes of transactions, we'll be required to review management's documentation and walk through a process. We'll need to take a sample selection of one or two items, walk through and see that we have a true understanding of the documentation. We'll have to make sure the documentation we've received is accurate, make sure the controls that have been identified are in place and, more important, look for what's not included on these things and what's missing from the documentation.

We talked about definitions of deficiencies. Enron and Andersen really came back to fraud. Interlaced with this is making sure that within all these key business processes, we've considered fraud risk factors and specifically identified controls related to fraud. You'll hear more about that as you hear anybody talk about 404 because it's part and parcel to the whole thing.

Let me talk a little bit about quarterly procedures. I think this is a bold statement: "If responsibilities are not fulfilled, the auditor should communicate in writing to the audit committee and disclaim an opinion or withdraw." It's a strong thought. I would like to think that in most cases we're not going to get to that kind of situation. I think we're trying to talk with management right now to make sure we don't get to a situation like that. We need to get on the same page about what the requirements are and move forward with that because that, in essence, is a scope limitation to us. If we don't think management's done enough work to support the assertion that it's making to third parties and to us, then how could we possibly issue an opinion on what we think about the controls? That's an important point.

Management's responsibilities include design of controls over all relevant assertions related to all significant accounts and disclosures in the financial statements, including all five components of the control environment. Another responsibility is providing information about how significant transactions are initiated, authorized, recorded, processed and reported. Again, that's interlaced throughout the standard. This isn't just that we do a budget to actual at the end of the period, so we're confident that we would have found any issues related to the accounts or anything that's material. That's not good enough anymore.

We have to get down to the transaction level and document the controls or initiation authorization recording processing and reporting. If there's one common theme to discussions I have with management, it is a belief that this is more high level than it actually is. It's at a fairly granular level, and there's a level of reason and materiality, as we talked about, that's going to be out there. But it's a large

process, maybe larger than many people will think it should be, but, nonetheless, it is what the standard requires.

Now I'll get to the auditor's responsibilities. Obviously we have to plan an audit, evaluate management's assessment process as part of walk-throughs and other inquiries and observations, obtain an understanding of the internal control and evaluate design effectiveness. We're following right along with what management has done. We're going to understand the control environment. We first have to say, "Based on our understanding of how this works, do we think, if it's in operation, it would be effective?" If the answer is no to that, you go back to the drawing board. There's no reason to start doing testing if you think it's not going to work, if it's not going to accomplish the objectives we set. That's where you have to start, right there, and then if it's not effective, you want to remediate those controls and get to something that's effective so you can begin testing.

It sounds like it's a linear process. In fact it's a more iterative process, and different processes have different determinations. Often you'll do some testing and realize some issues that you didn't know before, and you'll have to come back, remediate those and reassess the design effectiveness.

We have to test and evaluate operating effectiveness controls, consider how we can use the work of others in doing that, and then evaluate the deficiencies and form our opinion. On a quarterly basis, beginning in '05, we have to update those procedures.

Significant audit issues include scoping and coordination with management's process. It's all about communication, getting on the same page and getting over disagreements about scope. That's an important part of the process. Evaluating management's process, form and extent of documentation is always a hot button. My view of what good documentation is versus someone else's view may be different. It's another judgmental area that's out there.

How much testing and reliance on the work of others is another issue. Many larger companies have extensive internal audit departments. In some cases we in the past have worked closely with internal audit. The department has performed work on our behalf. We'll say for cash this year, we're going to have internal audit all the bank reconciliations. We're going to do what's called SAS 65 review of that. The rules of the game again have changed a little bit. The testing that internal audit may do for management is part of management's testing, and we can consider that just like we can consider any other testing of management. Given that internal audit is viewed as a more objective source because it's a little more independent from the actual processes, we can place a little higher reliance on the level of internal audit testing, but, again, that's another debated topic right now.

We talked about evaluating deficiencies. Evaluating the audit committee's effectiveness is a new and difficult item to deal with. It falls into the control

environment area, the tone at the top, and the effectiveness of the company's governance structure. Also evaluating controls over fraud risks is a significant issue.

We have to do our own testing. There's the concept of unpredictability that's thrown into the standard, and there's a lot of debate about this. I had this question from a partner last week. I said that you have to test all the controls every year. He said, "What's so unpredictable about that? They know I'm going to test everything every year. What's so unpredictable about that?" What the standard is talking about is varying the nature, timing and extent of testing year to year, and I think also what you'll see evolving is this use of the work of others concept is going to be part of that process. If we're using the work of others, we may use it more in one place one year and less in another year. While the word "rotation" I don't think is going to be the right word going forward, we will need to evaluate that differently each year and try to have some level of unpredictability. That goes back to fraud and some belief in the past that the auditors have been too predictable about where they're going to be.

The high level of assurance needed is another big point that's specifically mentioned in the standard. What does that mean? Our firm's belief is that's to a 90 percent to 95 percent confidence level, and that will drive what we believe the level of testing is, and some tie into statistical validity of testing. When you see or hear about PWC sample sizes, and I believe most of the firms are coming close to each other on this one point as far as number of items. That's what we're trying to get to—a high level of assurance and a 90 percent to 95 percent confidence level in that testing.

A consideration we talked about earlier was the nature of the control—manual versus automated, frequency of operation and importance. These are all factors that will determine the level of testing. Clearly, manual controls would have more testing around them than automated controls, and the more often they're performed, the more often they should be tested. You should test multiple locations under business units. I think probably most of the companies that you're familiar with, especially the larger companies, have a number of different systems, different processes and different locations. You have to evaluate them and determine what level of testing you're going to do.

From an actuarial perspective, this is one I've seen debated recently: What's a third-party actuary? Is that a service provider or an expert? I think the stock answer is that if you have an actuary doing valuation services, that's a person doing an expert service, and that's scoped out of the service provider guidance. The concern I think some people have is that reserves and the cycle are such a big part of a an insurance company's business, so would there be an incentive for companies to come up with an approach that maybe in substance doesn't change much but moves the actuarial function outside of the company to scope it out a 404? It's not inconceivable that you could have something like that occur but not have a real substantive change. That's one that I think may be a facts and circumstances type of deal, but it may be an interesting one to watch evolve over

the next couple of years.

In evaluating deficiencies, we have to look at the likelihood and magnitude. The definitions of likelihood and magnitude probably depend on whom you ask. FAS 5 does give some ideas about this. Probably the closest you have to anything in the literature out there is Staff Accounting Bulletin (SAB) 99 and some indication from the SEC that 5 percent of pretax income and above is material. If that's material, then what's significant? Those are tough questions that we'll all be dealing with. Probably it will be a number lower than most people think it is. SAB 99 talked about quantitative. The 5 percent is a quantitative measure. Other qualitative factors may be other things that should be considered within a particular industry that might be considered material.

Here are some indicators of significant deficiencies that might be material weaknesses. The first is a restatement of financial statements. If we identify material misstatement prior to management's controls identifying them, that's probably a material weakness. The next indicator is ineffective oversight by the audit committee. Other indicators include anything that involves fraud and senior management; that fraud concept is embedded in there.

Other deficiencies that are probably at least significant deficiencies include a company's not having an effective control over selection and application of accounting policies. That's a big problem if it doesn't have any fraud programs and controls or if it doesn't have sufficient ones. Controls over nonroutine and nonsystematic transactions are important. This gets back to fraud because these are nonretain things. They're more susceptible to fraud risk. A big one is controls over the period-end financial process, the actual aggregation of all this information into consolidation—the general ledger, the journal entries, things like that.

These are particular areas of concern. You should have time to remediate the control issues that Ray talked about a little bit earlier. You should get on these quickly and identify them early enough before year-end so that you can have them in place and tested. The financial reporting process is a huge one that auditors have relied on controls in. We've always done substantive procedures in those areas, and so it's not one that's well-documented.

Spreadsheets, again, are a hotly debated topic. There's a lot of concern over spreadsheets in the actuarial world. We believe that there should be some higher level of control around those as they exist today. What does that mean, and how's that going to be defined? That's still being debated.

Other areas not traditionally audited for controls include actuarial and tax. We've taken more of a substantive approach: Did you get it right at the end of the day? We didn't focus on controls. I think we talked about nonstandard journal entries. For acquisitions close to year-end, we may be getting some relief from the SEC on this to be able to limit our scope in some cases if we have an acquisition toward the

end of the year. There will be more to come on that.

Once you have one of these weaknesses, especially a material weakness, how are you going to report that? What does it mean to the companies that have material weaknesses and adverse opinions? In the past, as an auditor, the SEC wouldn't accept an adverse opinion on a set of financial statements. It'd block your access to the capital markets. It's said in this case it's not going to. You can have an adverse opinion and still participate in the capital markets, but what does that mean to the company? What does it mean to your share price and public perception? I don't know if I can tell you the answer to that question today, but we'll know by this time next year, I think, what the answer to that is because we expect there will be companies that will have material weaknesses. Time is not on our side.

MR. R. THOMAS HERGET: I think you did a fine job presenting Sarbanes-Oxley in a general context. Could you comment about what you might see coming up for life insurers? After that, what do you see coming up for actuaries within life insurers as far as complying with Sarbanes-Oxley?

MR. ZIMMERMAN: I'm on AEGON's Sarbanes-Oxley project management office team, and our actuaries have been heavily involved in the documentation of the processes. We are currently instituting a number of remediation policies in order to formalize our controls. Spreadsheets were a big issue. We've come to the conclusion that we're never going to have controls around our spreadsheets that would meet a Sarbanes-Oxley definition, and so the key control will have to be review of the results.

We ask the actuaries, "How do you know the review is right?" They respond, "Professional judgment. Leave me alone." We say, "That doesn't cut it anymore. You need a way to formalize your review, write down what your expectation is, why you believe it's that and then look at the number and tell us whether it's in your expected range. If it's not, investigate it and explain it." There's going to be a lot of work for the actuaries. Does anybody have any other color to add to that?

MR. IRICK: I would agree, but somebody kept mentioning how granular this thing is. The only way that you're going to be able to continuously update this on a quarterly basis is if you have people living and breathing this day to day. You're going to have all these processes owned by somebody. I suspect that there's going to be somebody within actuarial who's going to own a lot of the actuarial processes and who's going to be responsible for updating this and reporting issues.

MR. MILES: The only thing I'd add is documentation around these processes. A lot of things may be part of what you do on a regular basis, but it's another thing to try to get some of the things you do on a regular basis on paper to show what you've done. It might require going back to the old days when we used to initial things, say when we did them and say who authorized them. That's what a lot of this is about, and I think that will impact. Auditable evidence will be important. I'm

not sure if it's part of your question, but Ray alluded to the NAIC debate. If you want to call it life insurance just as an insurance industry, the NAIC, I expect, is down a path that it'll never return from, which is going to end up in a Sarbanes-Oxley-type requirement for individual insurance companies to some degree. I'll be interested in your thoughts. It's a little way down the road, but I think it's a reality, and it will be a big issue for the industry.

MR. SMITH: I think what the NAIC is looking at is ever since the Financial Institutions Recovery, Reform and Enforcement Act (FIRREA) or Federal Deposit Insurance Corporation Improvement Act (FDICIA), the banks have been doing internal control reporting for regulatory purposes for a few years. I think the banking regulators gave them a couple of years to comply and made it applicable to fairly sizable large organizations. I think the $25 million or whatever that's in the model audit rule draft that's out there today for 404 has to move. The applicability to separate legal entities is going to be a struggle, particularly for AEGON. There's a history of the banking regulators having done it, and I'm sure the insurance regulators will ask why not.

MR. IRICK: I think they get a no-material-weakness letter from us, look at the fiduciary requirements in Sarbanes-Oxley and realize this thing doesn't say anything. To be honest with you, it basically says, "If we happen to stumble upon a material weakness, we'll tell you about it." When I first saw this coming down, it seemed like a natural thing to come down the chain later on down the line.

MR. ZIMMERMAN: I have one warning: About two weeks ago I was talking with somebody who finally had a full appreciation for the magnitude and the seriousness of Sarbanes. Here is one thing that has changed from the former audit process. If you got into January, were rolling up your numbers and found a mistake, it used to be enough to just fix it. If somebody was doing some testing of what would happen if valuation rates went down to 4 percent, was playing around in the model, and the model had some bad results. he'd book the number. Somebody would say, "You know, this just doesn't feel right. Check into this again." It was an informal control that would have caught the error of a bad valuation rate or something like that, and at that point there's nothing you can do. It's not enough to have the right number; a mistake got through, and it wasn't caught by any of the formalized controls. You're getting an adverse opinion, no ifs, ands or buts. It's serious.

MS. REBECCA CONWAY JUSTICE: I have a question about what other companies are doing about the controls around reserve calculations that are done by a system such as PolySystems.

MR. ZIMMERMAN: AEGON has taken the position that, for the actuarial systems, it's not cost-effective to put in the framework that a general computer control regime would have. It's expensive, it's bureaucratic, and it's just not cost-effective for the four or five actuaries who are using these systems to put those types of controls around this. If you formalize the review process of the reserves or your

DAC or whatever the reserves are afterwards, we're of the opinion that that's our key control for ensuring that the calculations are accurate, and, therefore, we don't need the prohibitively expensive controls that a general computer control regime would have. You might want to talk to your auditor about that.

FROM THE FLOOR: I think the key thing with systems such as PolySystems is that the actuary has to test the results some way. He has to make an effort to ensure that the input went in right, and the output's coming out right. He has to do some independent testing of the system. He can't say that every calculation is right, but he has to demonstrate that he has some confidence in the system by doing something himself. I think that's an important issue. Systems are getting more and more complex. People are less knowledgeable about the basics, and if they don't test, then they don't know what they have. To say that the system is widely used is not a good enough answer.

MR. ZIMMERMAN: Documenting who has controls to the files, maybe password protecting some things, using signoffs when files are changed (you update premium factors, for example), documenting that they've been changed, noting who changed them and when they were changed, and documenting that testing was done to ensure the right factors were put in saves you a lot of upfront testing.

MR. MILES: General computer controls around that particular application definitely apply. That's not to say that you wouldn't take a hard look and test some of the output. Making sure that they track back to the administrative systems is a perfect step, and if you have reconciling items where the interface isn't necessarily working, make sure that you timely clear reconciling items, timely clear differences and timely clear suspense items. It's not just one step to reconcile things. You have to go in and deal on a timely basis with what the reconciling items are for the controls not working.

MR. ZIMMERMAN: I would agree with that, but I'd like to clarify my earlier comments. I'm not saying don't have any controls because you're not going to get credit for it. It's almost like the exam process. There are things you need to know to do your job, and then there's this other set of things that you need to know in order to pass the exam. You need to have a system, test it, maintain the documentation and have a test plan. That may be a key control that should be audited. But the level of controls that you need is a cost-benefit analysis performed by management, and for a general administrative system the controls will include limited access. You need to submit a change request for anything you want, and the actuary has to submit user specifications. There must be a formal test plan, and it must be tested in the test environment first. It's not cost-effective to apply that type of a control regime to PolySystems. If you did have the general computer controls around PolySystems, you could take the answer from it with absolute certainty that it is right and book it without reviewing it. AEGON is not ever going to get to that level of controls with our PolySystems. It's the review that we're relying on.

MR. MILES: I think Brad mentioned that you have to evaluate and test controls each and every year, but on some applications the concept of benchmarking still applies. If once upon a time somebody went out and made sure that the calculations all worked, but then after that point we rely on change management controls and access to those systems controls, at least that's the position I think we're taking on some applications. You can benchmark them one year and then track the security and access controls and change management controls.

MR. IRICK: It goes back to the comfort level that Darin talked about. How willing are you to get burned at the end of the year when a mistake's been made and you get an adverse opinion?

Chart 1

Process Overview

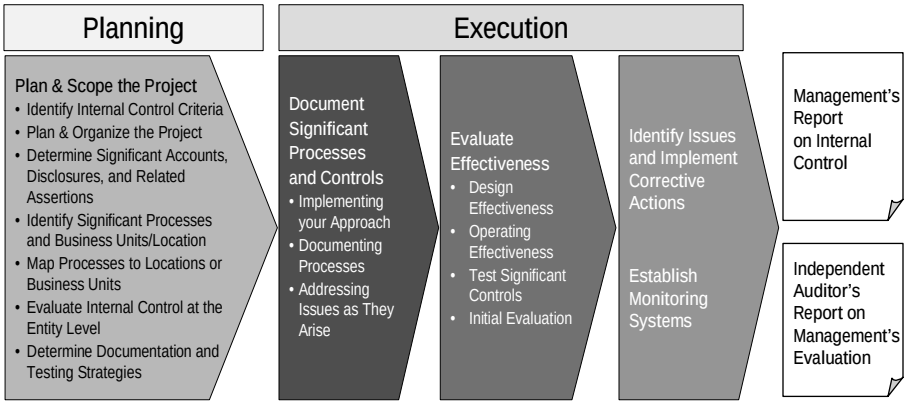

Chart 2

What is Internal Control?

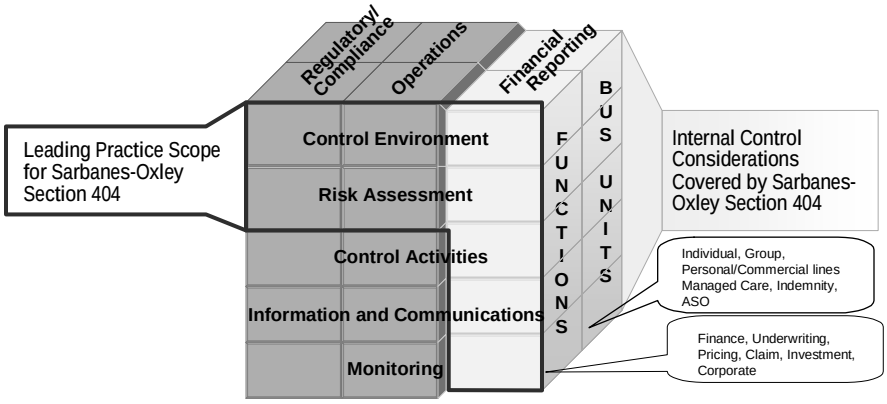

Diagram Based Upon AICPA Auditing Standards AU319, Definition of Internal Control (Paragraph .13)

Key Insight

- Leading companies are using Section 404 compliance as a catalyst to review their entire risk framework

Chart 3

Process, Transaction or Application Level Control Evaluations

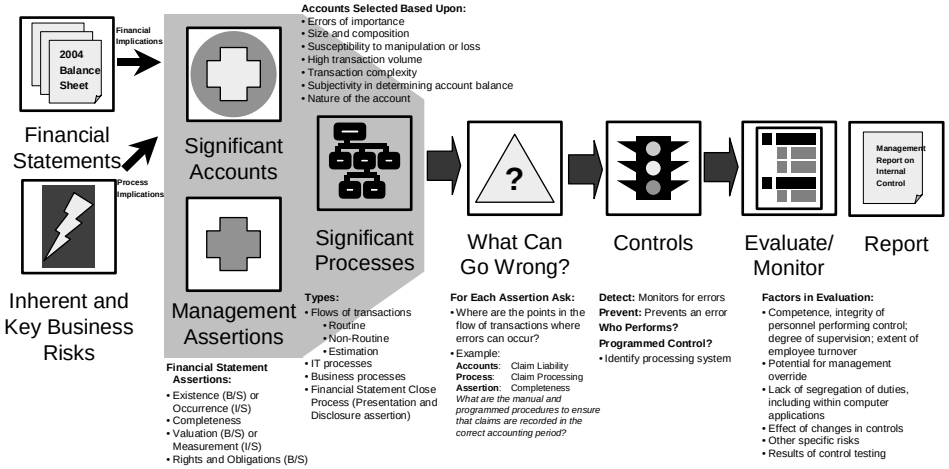

Chart 4

Sample Project Team Structure

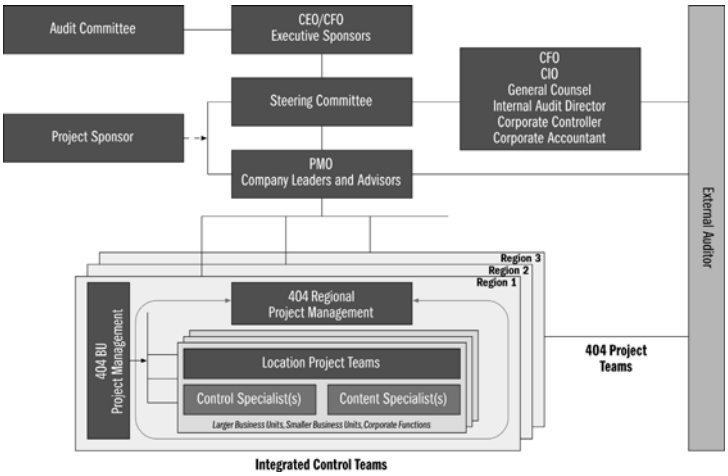

Chart 5

Key Issue: What Technology Enablers are Being Used?

- Of companies that have selected a vendor
  - Risk Navigator was most often selected
  - Other tools included On Project, Open Pages, Handy Soft, and Movaris
- Some companies have built or converted in-house systems