Comptroller of Currency

Administrator of National Banks

Audit Roundtable, Part 1

Risk Assessment and Internal Controls

Thursday, November 15, 2001

9:00 a.m. – 10:30 a.m. EST

Jim: Today's program is sponsored by the OCC, however the views of the outside presenters do not necessarily represent the views of the OCC. Today's seminar is entitled "Risk Assessment and Internal Controls" and will be hosted by Mr. Zane Blackburn, Chief Accountant for the Office of the Comptroller of the Currency. But before we get to our panel and introduce our speakers, I'd like to introduce the Comptroller of the Currency, Mr. Jerry Hawke.

John D. Hawke, Jr.: Good morning. It's a pleasure to welcome participants from all around the country to the OCC's Audit Roundtable, the latest in a series of teleconferences that the OCC has sponsored over the past year. Thousands of people like yourselves have found these forums a useful and cost-effective way of obtaining up-to-the-minute guidance on a wide range of supervisory issues. Indeed, some of you are back with us for the second or third time, and we really appreciate your interest and support. The subject we're addressing today is certainly among the most important the industry faces—too important, in fact, for our discussion to be contained within a single session. Accordingly, our Audit Roundtable will be continued on Thursday, December 13, and conclude on Wednesday, April 3, 2002. We hope that today's program will encourage you to sign up for the others in the series.

The importance of the audit function for bankers, bank directors, and regulators can scarcely be overstated. Internal audit is a key element in any effective program of internal controls. To the directors and shareholders, the external audit is a crucial source of independent and expert insight into a bank's true condition and the integrity of its systems. And for the OCC, the strength of a bank's internal and external audit functions strongly influences the kind of supervisory scrutiny that we provide. When we identify

weaknesses in a bank's audit in internal controls, we necessarily increase the amount of validation and testing of bank operations that our examiners perform. Conversely, the finding that a bank has a robust and reliable audit program enables us to step back and allow these processes to work with minimum interference on our part.

In challenging times such as these, audit and internal controls loom larger than ever. Banks are under more intense cost-cutting pressures today than they have been in many years. It's an unfortunate reality of corporate life that functions, as contribution to the bottom line may not be immediately evident, are often first to feel the pinch. Even large institutions have taken to outsourcing their internal audit, raising a host of new issues and concerns. How banks can deal with these pressures without cutting corners or compromising the reliability of their audit and internal controls will be among the many topics we'll be covering in today's teleconference.

Although the topics we've dealt with in our telephone seminars have ranged widely, they've all been based on a belief in the importance of good communications between regulators and the industry. Our common interest in a safe and sound banking system requires that we understand each other's needs and perspectives. And I believe that our ability to exchange views and information in forums like this one materially advance that goal. I wish you a successful seminar and thanks for being with us.

Jim: Alright, thank you, Jerry. And at this point we'll turn things over to Zane Blackburn.

Zane Blackburn: Good morning. I'm Zane Blackburn, chief accountant at the OCC. The primary purpose of these Audit Roundtable sessions is to reemphasize the importance of strong audit and internal control programs. Moreover, we believe these

discussions can assist bankers, examiners, and external auditors in helping us achieve our objectives by having a better understanding of each other's audit and examination approaches. Understanding each other's respective objectives will also help us accomplish them in the most timely and effective manner. From our perspective, and I would assume from yours as well, internal control is the cornerstone of risk management. The effectiveness of risk management is key to the safety, soundness, and success of every institution. I am sure you may also agree that revealing and testing those controls through rigorous, independent transaction testing is key to the objectives we each seek. With new products, services, delivery channels, and other economic uncertainties taking place in the banking environment, it's increasingly important that bank managers and directors heighten their oversight of audit and internal control systems to ensure they are effective. As we all know, effective internal control and audit programs are essential in safeguarding assets, assisting in the timely detection of operational errors, and producing accurate bank records and financial reports. For these and other reasons, our examination staff will focus on the adequacy of the individual bank's audit function, both internal and external as well.

Today's Audit Roundtable will focus on risk assessment and internal controls. We strongly urge you to participate during the question-and-answer session so that we can all receive the maximum benefit from those questions.

Wynne Baker, chairman of the AICPA's financial expert panel, will give some brief opening remarks, followed by our presenters: Bill Lewis who's a partner with PricewaterhouseCoopers and Matt Lusco, a partner of Andersen who is substituting for his colleague, Craig Dabroski. Before we begin, Jim, do you want to go ahead and do an attendance poll?

Jim: Yes, I would. At this point we would like to determine just how many people are attending today's seminar. If you are attending alone at your site, simply press the number one on your telephone. If there are two people at your site, go ahead and press number two. Press three for three people and so on up. Now if there are nine or more people at your site, simply press the number nine on your telephone keypad. You can go ahead and register in those numbers now. Once again, press one, if there's one person at your site. Two, for two people. Three, for three people and so on up. If there are nine or more people at your site, simply press the number nine on your telephone keypad. We'll have those results for everyone in just a little while. At this point we'd like to turn the program over to Mr. William Lewis. Bill?

William Lewis: Jim, thank you very much. It's my pleasure to be here with you-all this morning for this important conference call. And I'd like to start off by talking about our approach to today's presentation from a standpoint of risk assessment, sampling, and materiality. I'd like to echo Zane Blackburn's comments that we believe firmly that it's important that each of the parties to an audit of the financial statements understands clearly the other's approaches and objectives. While our primary constituents in performing an audit of the financial statement are the shareholders and the audit committee of the bank that we're auditing—as well as the management of that bank, it's important for us to know what others are interested in, in terms of the objectives of their work, so that we're aware of areas where our work might coincide with theirs and their expectations as we deal with them.

Today I'm going to be talking about risk assessment, sampling, and materiality in a financial statement audit. A financial statement audit is one of several types of engagements

that an independent accountant might perform for management. But my comments will be limited to that. It is important to note that there may be instances where auditors are called upon to do special internal control reviews, director's examinations, or other types of work—attestation types of work—for audit committees and management of banks. And they would result in different risk assessment and sampling and materiality considerations. The objective of an audit is obtaining reasonable but not absolute assurance that financial statements are fairly stated. And in doing that the most important part and fundamental part of the audit approach is the risk assessment process. In assessing risks, auditors consider three different types of risk: two of them relate to the client's business and the other really relates to the combination of the risks identified in that process and the auditor's own risk profile.

Let's talk first about the client business risks. First is inherent risk. An inherent risk is a risk category that really relates broadly to the activities and operations of a company without considering necessarily the company. For example, unsecured lending is inherently more risky than secured lending. If I were auditing an institution that was primarily involved in unsecured lending, then I would have a higher assessment of inherent risk in that organization than, let's say, secured lending. And that's a fairly simple example, but that type of a risk assessment is done for each critical business component.

The second type of risk that an auditor considers is control risk. The control risk is the risk that an institution may not put in place the checks and balances needed to mitigate inherent risks and other operating risks that an organization has. So it's an assessment of how much inherent risk there is, and how much management has done to put in place controls to control risk.

That's a fundamental building block of risk assessment for an auditor.

The other element of risk assessment is important for an auditor. And that is the assessment of audit or detection risk. An audit or detection risk is just a basic business risk for an auditor. It's the risk that the analysis and the work performed by an auditor may unknowingly lead to failure to detect a misstatement in the financial statements. And that can occur simply because of the procedures and the methods the auditor uses to make his or her risk assessment or the evidence of fraud, which might not be detected by an auditor.

Let's talk now about the causes of risk. The primary causes of risks are complexities, errors or misjudgments, fraud, or misappropriation of assets. Complexities are a very important part of the risk assessment process. Obviously if an institution has more complex business operations, is involved in transactions that have a higher degree of subjectivity or estimation risk from a standpoint of applying generally accepted accounting principles, or has a wider breadth of operations, then risk will increase, while more routine and simple operations will have lower risk.

Errors and misjudgments are an important part of the assessment of risk for an auditor. I'd like to make a distinction between errors or misjudgments and fraud. Errors or misjudgments involve mistakes such as mistakes in gathering data or mistakes in applying generally accepted accounting principles. They can also include unreasonable accounting estimates that result from oversight or misinterpretation of either data that's been presented or the methods that generally accepted accounting principles use to translate that data into accounting results. The key here is that those are unintentional acts.

Fraud, on the other hand, is an intentional act to misstate the financial statements—whether it's done through data manipulation, through intentionally arriving at estimates that are different from the real estimates that should exist for the financial statements, or the intentional misapplication or indifference to generally accepted accounting principles. Those key elements are important for an auditor to consider in making an assessment of risk. If there's been evidence in the past of a large number of mistakes or errors or if there's been evidence in the past of management fraud, then the auditor will have a heightened assessment risk and will appropriately tailor his or her procedures in light of that.

In the risk analysis approach, there are several key considerations. One is the identification of inherent risk of material misstatement, that I talked about earlier, by understanding the business. The next is understanding the control environment that management has placed into action in order to—for its own purposes—mitigate that risk.

The next is the evaluation of any remaining risk that might exist, that's peculiar to the institution. The next step is the development of an audit approach. And we'll talk briefly about that in a moment. The audit is a cumulative process. It involves a continual assessment of risk. Risk assessment is not just done during the planning phase, but is entered back into the equation at several points during the audit process.

Let's talk for a moment about inherent risk identification and what the key steps are in performing that task. The first is to understand the nature of the client's business. Inherent risk will vary by client, and the approach taken to assessing it will vary by client. It's important that an auditor maintain constant communication with management to understand changes in the

business that would affect its inherent risk assessment. For instance, if management entered into a new line of business or entered into significantly new and perhaps higher-risk products during the year, it would be important for the auditor to maintain communication to understand that and to, as timely as possible, enter that into the overall risk assessment.

The next area that's important in risk identification is understanding reporting complexity risk. And what that means is how generally accepted accounting principles and what generally accepted accounting principles apply to the client's activities. For instance, if an institution is involved in a significant amount of hedging, particularly hedging that involves use of unconventional instruments or involves a high amount of likely ineffectiveness, then there's potentially a huge amount more of reporting complexity risk than at an institution that would not be involved in FAS 133. Same with asset sales securitization activities and other activities that involve very complex accounting standards such as FASBE Statement 140.

Another important and inherent risk identification is understanding industry trends. For instance, one key factor is monitoring industry activities through audit risk alerts produced by the AICPA, banking circulars and bulletins issued by the regulatory agencies, speeches, etc., of the regulatory agencies and the FCC to understand key identified risks by those parties and actions that are being taken by them to react to them. Key regulatory issues are important in risk assessment, not necessarily for an auditor to begin testing specifically for compliance with laws or regulations nor to report on them, because that's not an objective of the basic audit. But it is important for an auditor to understand key regulatory issues to consider the risk of whether noncompliance with such laws and regulations could have a

material effect on the financial statements. To the extent they could, then the auditor must factor that into their determination.

The other consideration in inherent risk identification, frankly, is engagement-team expertise. Audit risk, as I indicated earlier, is the risk that an auditor may fail to detect risks and fail to detect, therefore, material misstatements in the financial statements. Before undertaking an engagement in a highly regulated and specialized environment such as banking, it's important that an auditor have the proper engagement-team expertise to make the right risk assessments on inherent risk. An auditor then, under generally accepted auditing standards, is required to document the specific inherent risks that have been identified, assess the risk of fraudulent financial reporting, and the likelihood that that financial reporting could result in material misstatement; assess the risk that management or others from the outside might have inappropriately misappropriated assets of the entity; and use all of those considerations to develop an audit strategy with factors relative to those inherent risks.

I'd like to move forward now to talk about the control risk assessment, which, you may remember, is the second client-facing risk assessment that an auditor needs to do. Control risk assessment is one of the more pervasive risk assessments done at the beginning of an examination. And its goal is really to try to assess the procedures and the policies and the actions that management has put in place to address inherent risk in the business and to mitigate the risk of material misstatement in the financial statements. A control risk assessment is something that should be viewed from the top down. It's important, as Comptroller Hawke noted earlier, that management take a leading role in establishing internal controls in their organization, to

control against not just financial reporting risk but operating risks and compliance risks.

And while in a financial statement audit we're primarily focused on financial reporting risks, many of these activities, I'm going to talk about in the next few minutes, mitigate the risk not only of financial reporting misstatements, but also of operational breakdowns or compliance failures. Important is the tone at the top, and the role of the board of directors is critical to that. The delegation of responsibility, the setting of the establishment of policies, and expectations for management to maintain compliance with those policies is critical to the culture, the control culture in an organization. The effectiveness of the organization and key management is also important. If reporting lines are structured in a way that management fails to communicate properly, fails to identify risks, or is otherwise dysfunctional, then it's important for an auditor to identify that—factor that into its program. Also human resource policies and procedures are important in that they are ways in which people are measured and which drive the behavior of employees. If human resource policies and procedures do not reflect appropriate levels of accountability in staff, then there's a risk that those accountabilities may be not taken seriously and could lead to heightened control risk.

It's also important, after an auditor assesses the overall organization and roles and responsibilities of the key players, that they try to determine what management's risk assessment is. One of the things that the banking regulators have tried to do in the last several years is to align risk assessments. And that's something an auditor tries to do as part of its engagement. And to determine whether the risk assessments that the auditor is making are consistent with those management has made. And particularly they'll inquire of management of areas where there have been past

reporting deficiencies that arose either from prior audits or from examinations by the regulators, in terms of regulatory reports. We'll also press management carefully on the processes management uses to determine their own estimates of accounting judgments and the planning process management puts in place to mitigate and monitor controls. Budgetary controls are often an important part of that, in that that's the way that management ensures that they track the financial results and operations of the company.

Monitoring controls are also a critical control to consider. And the important parts of monitoring, and they'll vary bank by bank depending on size, are: the role that the audit committee plays, which is critical in any environment; the role that internal audit or a separate compliance department might play in monitoring compliance with laws and regulations, as well as with the internal controls that management has put in place; the change management process that management has in place to ensure that, before a new product or business venture is entered into, that there's an adequate consideration of the risks to financial reporting that might accrue.

Business line-level management monitoring processes are important as well to the auditors because many of the tests that the auditor will perform will be at the component level, let's say in particular departments such as deposits or loans or investments. And so it's not just the tone at the top and the overall management controls, but also the line-level monitoring controls. And then just a very qualitative judgment on the part of the auditor, in terms of the integrity and ethical values that management has displayed in its years of association with the client. And considering all of these, the auditor will come to a determination of whether or not control risk—this one element—is high, moderate, or low. If

control risk is high, then controls will likely not be relied upon and a more substantive approach will be taken to the audit. In other words, the auditor will try to test balances and do more third-party confirming-type tests than testing of controls and relying on them. However, if the risk assessment is low, then controls will be relied upon and controls will likely be tested as a basis for determining whether financial statements have likely been materially stated.

Next, I'd like to talk a bit about the analytical procedures that are put in place as part of the next step after control and inherent risk is determined. Analytical procedures are used to identify changes in the business since the last time the auditor made an assessment. And analytical procedures will focus on balances, results of operations, and other key quantitative indicators that management has in place to run the business. Next, the auditor will determine whether or not the transactions that are in vogue are homogenous and routine, or whether there's a large amount of nonrecurring, unusual, and complex transactions. In a situation where the latter exists—that large, nonrecurring, and unusual transactions or highly complex transactions will likely have a material effect on the financial statement—it's not atypical for an auditor to divert much of its attention to those large transactions and to do specific transaction-level testing to ensure that they've been properly accounted for, and then place perhaps less emphasis on the need for more detailed control testing.

And a very critical part of the analytical procedures and requirements under generally accepting auditing standards is the assessment of materiality by an auditor. As I've indicated earlier, material misstatement of the financial statement is something that results in a different opinion from an auditor and really is critical to the principal audit objective. As I indicated earlier, I differentiated between errors and frauds; the actions that an auditor takes with

respect to both also differs. Materiality is invoked when errors are found—unintentional mistakes. A minor misstatement is something that may not be significant to an audit and to the opinion that the auditor needs to render. And the response the auditor will take to that minor misstatement is going to be less, and will likely be simply to bring it to management's attention—if it's considered to be an isolated and not a pervasive issue. However, if fraud is identified—even a minor fraud gets high attention, because there's a possibility that a minor fraud might be an indicator for a broader integrity issue with management. So, with a minor fraud identified, there is no materiality in terms of the requirement of an auditor to report it to management and to the audit committee. Materiality will be affected—the judgment used by the auditor will be affected—by the size of the institution. And audit to audit, it will also vary, depending on changes that have occurred in the business and in the internal environment.

Planning stage materiality considers the control environment, the size and complexity of the entity, and the cumulative experience that the auditor has with management, in terms of the way it acts in reaction to errors or mistakes that have been identified in the past. It also recognizes the inverse relationship between materiality and audit risk. Low risk, there is a low risk of large misstatements and there's a higher risk of small misstatements. The auditor must balance these, knowing that even a batch of smaller misstatements might not rise to the level of a material event that needs to result in the adjustment of the financial statements. So the auditor must consider what combination of large, low-risk misstatements and lower risk but potentially more numerous smaller misstatements might trigger the need for a determination that an adjustment needs to be made to the financial statement.

Based on that very judgmental assessment as well as an analysis of each financial statement—the income statement, the balance sheet, the statement of changes and inequity, and the statement of cash flows—the materiality level will be determined for each statement. The smallest aggregate materiality level among the misstatements should be the benchmark by which all adjustments that are identified, or errors or mistakes in the financial statements are identified, are monitored, and gathered in order to determine whether an adjustment needs to be made to the financial statements.

The estimate of likelihood of occurrence will be based on the experience that the auditor has with this entity and similar entities. In a pre-occurrence materiality amount for each transaction will be used to aggregate the items for consideration for overall materiality. Materiality must be assessed by an auditor both in terms of individual transactions and in the aggregate. And therefore it's important that they prepare themselves to be in a position to make that assessment. As I mentioned earlier, materiality assessment is not a one-time process, but it can change during the audit. For instance, the number of adjustments found in testing might lead the auditor to reassess the level of materiality and the size of items that need to be gathered for overall assessment. Also variances in the financial statements or in the business during the course of an audit could also lead to a change in those assessments. I'm not going to talk today here about materiality in the wrap-up of the audit, as that's going to be covered on next month's session by a different presenter.

Lastly, I'd like to talk a little bit about the methodology used for actually doing testing. The ultimate judgment as to what needs to be tested after these risk assessments and materiality assessments are done, in order to render an opinion, rests solely

with the auditor. The determination that will go into this will include the relative risk of the individual item to the overall financial statements. And also we'll consider the nature and the purpose of the test that's being performed. If the nature and the purpose of the test is a substantive test, the auditor will likely have less tolerance for adjustments or items that are found. If it's just more of a control test, there may be certain tolerances that are built-in for errors. But once those tolerances are reached, then it's likely that the auditor will have to do more testing to satisfy themselves.

One area where there's often confusion among auditors, examiners, and even the banks that they audit is how auditors go about making sample determinations. It's important to know that the ultimate determination of a sampling method and sampling size rests with the auditor's judgment. Sample-size determination needs to be differentiated from sample selection or from statistical evaluation or results. An auditor has the ability to use, whenever they want, judgmental sample sizes, determining how many items they need to test in order to reach a conclusion. The way that they determine a sample size can be judgmental or statistical. Further, the way that a sample is selected can be handled in a way that is random or nonrandom. And finally, the way that evaluation of results occurs will also be determined based on the way that the sample-size determination was made. The auditor will not be able to reach statistical conclusions unless they have properly decided sample sizes and selected samples using statistical and random approaches. Again the determination by the auditor as to what types of sampling techniques to use in which instances will depend on their overall experience with the client, their auditor judgment, and also the type of tests that they're doing.

Transaction testing typically can take two different types. Testing of attributes, which is more of a control-type test where an auditor might select a series of items to test the number of key controls that are important to the processing and recording of transactions. That type of approach would typically be taken when an auditor is placing a higher level of reliance on controls.

Substantive testing of balances might also use sampling. And it would also look to quantify the results that are achieved from the sampling, in order to try to extrapolate the results from the sample to a potential adjustment to the overall financial statements. Again, the auditor's judgment, the past experience with these sampling techniques, and the degree of monitoring that management puts in place over controls will help determine the overall approach used by the auditor.

That wraps up my presentation for today. I'll be pleased to handle any questions we might have. Jim, I'll turn it back over to you.

Jim: Alright. Thank you very much, sir. At this point I would like to give the results of the first polling question that we did. We have just under 900 people attending today's seminar.

We also would like to do a follow-up polling question as well. And we'll have these results here in just a little bit. Which of the following categories best describes your company? Press one, if you consider yourself a financial institution. Press two for a public accounting firm. Press three for law firm. Press four for regulatory agency. Or press five, if you consider yourself other than what was listed above. And you can go ahead and press in the appropriate number now.

Again repeating, what is or which of the following categories best describes your company? Press one, financial institution. Press two for public accounting firm. Press three for

law firm. Press four for regulatory agency. Press five for other. And again we'll have those results here in just a little while.

At this point in the program, we'd like to turn things over to Mr. Matthew Lusco. Matt?

Matt Lusco: Jim, thank you very much. I, too, am very happy to be with you-all this morning. And echo the comments of Comptroller Hawke and Bill and others who have commented on the importance of a robust communication among all parties concerned, ranging from audit committees, management, external auditors, and, of course, examiners, as well, in this process. And I'd suggest to you that perhaps a primary forum for that communication exists as a result of auditors' responsibilities and management's responsibilities under the FDIC Improvement Act for reporting on internal control. And that's the primary area that I've been asked to comment on, which is internal controls and FDICIA, specifically management's assertions and the roles of external auditors in that. A couple of follow-on topics, too, that would be the issue of findings as it relates to evaluation in internal control, material weaknesses versus reportable conditions, the external auditor's role in reporting on fairness of regulatory reports, and, as Bill touched on to some degree, some additional discussion of substantive testing.

So opening up with FDICIA—since 1993, FDICIA has required, specifically one of Section 112 has required, bank management to evaluate and publicly report on internal control structure over financial reporting for banks. That requirement exists for banks with total assets greater than $500 million as of the beginning of their fiscal year. In addition to opining on bank financial statements, FDICIA also includes a role for the external auditors to examine and report on the assertions contained in management's report on the effectiveness of internal control over

financial reporting. Now, reporting guidance for the independent auditor is contained in the AICPA's Statement on Standards for Attestation Engagements, No. 2. FDICIA, however, allows management to define the elements of an internal control structure upon which its assertions would be based. But in accordance again with Statement on Standards for Attestation Engagements, the independent auditor can examine a report on management's assertion about the effectiveness of internal controls, only if management evaluates the effectiveness using reasonable criteria for effective internal control structures established by recognized bodies. And currently there are two acceptable sets of criteria for this public reporting on internal control. The AICPA's Statement on Auditing Standards No. 55 and the Internal Control Integrated Framework issued by the Committee of Sponsoring Organizations, or COSO, of the Treadway Commission. So all that undergirth, both management's assertion itself, as well as the internal auditor's responsibility and role with management's assertion. Now, as you can understand, this is evaluating and public reporting on the internal control structure, over financial reporting is actually a process or a pair of processes, both that undertaken by management as well as the independent auditor. And that process, I would suggest, is best discharged through close cooperation and very active communication.

The steps that management typically goes through is first an evaluation of the design and operating effectiveness of their own internal control structure of their organization. In connection with that it is important for management to review their information systems, general controls, as well as their overall regulatory compliance processes. In evaluating business process controls, which consist of the organization's process and monitoring controls, it's important for management to determine

and consider the nature, volume, and types of transactions for their various reporting areas, as well as considering specific—period-specific—economic events that have occurred in those areas. For each audit area transaction cycle, there are a number of different characterizations of units into which management and their auditors may break the organization down. It's important to identify key process and monitoring controls for all areas of the bank that will have a significant impact on financial reporting. And as a result of that identification, then to select process and monitor controls for testing. And that testing should determine that both that they are in place as well as operating effectively.

The next step in a process would be the design and execution of appropriate tests of these process and monitoring controls by management; the nature and timing and frequency of that testing should be based on the effectiveness of monitoring processes. And that testing for management can actually be performed by their internal audit organization.

The documentation of an evaluation of the operating effectiveness is the next critical step. And it will directly link to a conclusion on the overall design and operating effectiveness of the internal control structure and to ensure that that structure is both designed properly and is operating effectively to meet the preselected objectives that management will have agreed to. That's management's part of the process. The internal auditor's role will be to examine these assertions that's contained in management's public report, through meeting with management and agreeing on the significant economic events and the key transaction processes and controls and review management's documentation. Obviously, the quality of that documentation is important to consider the additional level of the external auditor's role in evaluating both the findings and what level of

documentation the external auditor will maintain to support their assertions along the way.

In connection with the examiner's role in the process, obviously upfront and effective communication is a best practice in this regard. The examiner should ask to see management's documentation and try to determine a comfort level with management's process, both from the objective and the documentation of testing. The examiner may also ask to look at the external auditor's work papers—that is provided for by FDICIA, for a couple of reasons. One, to see what the external auditor has done to document fulfillment of the responsibilities, as well as to see if the internal auditor has performed work to fill in any gaps in internal controls that may have been agreed to—both from management as well as the external auditor.

The types of documentation that are typically maintained to satisfy the requirements of the FDICIA and Statement of Standards on No. 2 would be documentation of the control structure at the overall level. And, as I've said earlier, that documentation should address both the design and operating effectiveness, documentation of the significant economic events that impact financial reporting, documentation of management's control risk assessment for each significant audit area, and that documentation should address the design and operating effectiveness of controls.

And finally, I think it's important to note that the bank will likely use existing documentation that they have in place. That documentation can take many forms to accomplish these objectives and could include their policy manuals, accounting manuals, procedures write-ups, flow charts, or any other level of checklist questionnaires that management may use to bridge their organization. I would suggest to you the key for that is the linkage of the documentation of management's evaluation of operating

effectiveness with the existing body of documentation that they rely upon and linking that with the control objectives of either COSO or SAS No. 55.

Finally, a topic that is of interest today, more so than at other times, are circumstances where an external firm may also be employed in an outsourced arrangement. And that can take a number of different forms, both in situations where one firm performs both the internal and external audit or where a pair of firms may be involved, or actually more firms performing various outsourced functions. I would believe the key consideration in those arrangements is the designation of an individual or a committee in the organization in the bank that actually takes full responsibility for the outsourced arrangement. To the extent that's in place and the independent standards of the performer are met, I would believe that it should meet all of the requirements for FDICIA to rely on the outsourced person involved in those organizations.

It gets a little bit more complex in certain environments where internal audit actually functions as a role in the control structure as opposed to simply auditing it. If that is the case, consideration need be given by both the firm opining on management's assertion on internal control and examiners to really evaluate what levels of dual responsibilities the outsourced party might have. In the same manner, I would suggest that if internal audit had a role in the internal control structure.

I'll break away and talk a little bit briefly about material weakness versus reportable conditions. SAS No. 60 provides the overall definition of material weaknesses, and it is incumbent upon an external auditor to report a material weakness. However, the reporting requirements for report conditions in material weaknesses under generally accepted auditing standards are fairly

open. They are required to be communicated to the client and to audit committees, but the nature of the communication is subject to judgment by the external auditor. It can be written; it can be oral. Often firms are asked to provide letters by audit committees or by external parties such as examiners, providing positive assurance that no reportable conditions or no material weaknesses exist. I think that you can understand that this is highly problematic, given that that would be a positive assertion and would require a level of auditing precision that's certainly not cost-effective and possibly even impossible to do.

In terms of the external auditor's role in opining on fairness of regulatory reports, call reports, that was discussed in the 1991 Joint Proposal for FDICIA. There was a push to require external auditors to opine on all reports. This was discarded and not pursued because of the variances of data that are included in call reports outside of external financial reporting and the significant levels of discretion required for reporting on various captions. So while the FDICIA responsibilities should include consideration of internal controls over financial reporting for call reports for regulatory reportings, the external auditor does not have a role in opining on the fairness of regulatory reports. And, of course, that would be a consideration for future legislative action.

As for substantive testing, Bill commented on the role of substantive testing, specifically analytical review in planning that is a critical element of substantive testing in the overall audit process. Substantive testing occupies a significant role in internal control analysis for FDICIA, as well as the external audit process, to cover circumstances of residual audit risk, where management or the external auditor finds a control gap where the control objective is not being met. It would be incumbent upon both management and the external auditor to deploy substantive testing,

which would be a more direct verification of account balances to backfill, if you will, where internal controls are not working. This is contrasted with compliance tests, which are audit tests, either through observation, inquiry, and other reviews of control documentation, to support the pre-selected test to determine operating effectiveness of the control structures, both for FDICIA compliance as well as performance of the external audit function.

That concludes my comments and I'll be happy to take other questions of the group.

Jim: Alright. Thank you very much, Matthew. And we'll get to Q&A in just a moment. I would also like to give the results of that last polling question. We had 80 percent of our audience today considers themselves to be a financial institution. So just to let everybody know again, 80 percent.

We would like to welcome aboard for the program, Mark O'Dell. Mark is the Deputy Comptroller, Bank Supervision Policy, Office of the Comptroller of the Currency. He will join us for the Q&A session, which happens right now.

By the way, if you do have any questions or comments to share with any of our panelists, all you need to do is simply press one on your telephone keypad. That brings you into the lineup here in our system. Now, when it's your turn to ask your question, I will call on you by the city and the state and the first name of the person who registered at your site. Now if your question is answered before your turn comes up simply press the pound sign on your telephone and that will take you out of the lineup. Here's a quick note for *[end of tape side A]* the speakerphone—it's best that you pick-up your handset when you ask your question. That way we're better able to hear you. And then as you are replacing that handset after your question, remember to press and hold that speakerphone button so you don't become disconnected. But if

you should become disconnected for any reason, simply dial back into the program, reenter your PIN number, and you will be reconnected to this program.

So remember, once again, if you do have a live question or comment to share, simply press one on your telephone; that brings you into the lineup here in our system. You can also ask your question via fax; simply send it in to me and I will ask the question for you. Our fax number for this session is 715–833–5469. And we do have a caller online, just trying to find my list here. And we will go to Denise in Houston, Texas. So, Houston, go ahead with your question or comment.

Texas: OK, my question is for FDICIA. Basically what I wanted to find is, is it safe, for example, for the investment cycle, we have done an internal audit of our investments, say in May or June of this year, and we went through the FDICIA assertions and most of it or all of it is covered in that audit? Is there a reason to re-do the FDICIA work at the end of the year?

Zane Blackburn: Matt, can you respond to that?

Matt Lusco: I can. I would say that there is not necessarily a requirement to re-do the work. However, depending on the risk that you'd identified through the risk assessment of the process and whatever level of specific and monitoring controls, it might be prudent or it might be appropriate to retest only the continuing performance of any monitoring controls that you're relying upon. If that's an important element of your control process, it is important, I think, to revisit performance of those controls, or to ensure performance of those controls, that operate during the period.

Jim: Alright, thank you very much, caller. And we will go on to River Falls, Wisconsin. And this is Laura's location. So, River Falls, go ahead.

Wisconsin: We have two questions. We're entertaining taking bids right now from external auditors for the IS audit. We want to know from the OCC, what are the specific requirements in terms of scope and the frequency of that? And then the next question would be what's the OCC's next hot button for internal audit issues?

Zane Blackburn: I'm sorry, this is Zane. I'm not sure what you're referring to as IS audit. Can you explain?

Wisconsin: Information systems audit, technology audit.

Zane Blackburn: And your question was, what are our expectations in terms from the OCC's perspective?

Wisconsin: Right. In terms of the scope and the frequency and exactly what's covered, because we're getting wide price variations in the bid cost for the audit.

Mark O'Dell: This is Mark. It's hard to give a specific answer without knowing all of the facts in your particular case. What we do when we look at IT audit, IS audit, or any audit, for that matter, is we look at the types of products, types of services that an institution will offer. We look at the complexity of the operations, how the control environment is structured, the kind of risk assessment that you do, and, based on a number of factors, our review of the audit function in IT and in operational areas will be influenced by these kinds of factors. So, the more complex the operation is, the more reliant on technology that you have in your risk management processes, and the more tailored products and services that you offer, we would expect that the control environment—the risk management process—would step up appropriately. And consequently we would expect also that, from an internal control or from an audit perspective, that the audit program, the internal controls, would reflect or increase in terms of oversight to reflect that increase in complexity, that increase in the

volume, the level, and the types of products and services that you would offer.

Zane Blackburn: Jim, let me just mention something before we go to the next person with a question. We have a number of bank examiners also participating in this call, and I would just remind them that they may certainly provide comments because this is a roundtable issue. And if they have questions as well for our audit speakers, they may certainly ask them. Do we have another question?

Jim: Yes, we actually do. I've got a faxed-in question here that came in during Matthew's presentation, so, Zane, I'll let you decide who should address this. But here's the question, "Why isn't the $500 million FDICIA requirement indexed?"

Zane Blackburn: I think the simple answer to that is it was a congressional decision and, unfortunately, as many laws that are tied to dollar amounts, very few are actually indexed.

Jim: Alright, thank you. And also, someone would like to, and I can do this, give Matthew's spelling of his last name and his title. It's Matthew Lusco. And Matthew is a partner with Arthur Andersen in Alabama.

Let's go to the telephones. We'll go to San Francisco, California. And this is Jim's location. So, San Francisco, go ahead.

California: Yes, I'm an examiner and I have a question about access to work papers. We often meet resistance on the part of bankers and especially on the part of external auditors and outsourced internal audit people to see the work papers for the areas that we're examining. Can you address the reason for the resistance and how to minimize the cost for the banks, when this has to be done to accomplish the requirement for the exam?

Zane Blackburn: Bill, I think you could either answer that or Wynne Baker as well.

William Lewis: Yeah, this is Bill. I would say that first of all our auditing standards and actually the FDIC Improvement Act provide that examiners do have access to review our work papers when they need to. So the groundwork, I guess the rules, are there to basically to, one, require that auditors to do it under FDICIA. And two, there are auditing standards—generally accepted auditing standards—that, and interpretations thereof that, guide auditors on how to go about it. None of which are really restrictive in terms of saying, "Don't let examiners review or in any way encumber their review." So the answer to your question is, there shouldn't be resistance here.

Now, that having been said, there are a lot of people who have had varying experiences over the years in terms of their work paper reviews. And I think it's really important that these requests be made in a way that expresses the expectations and the reasons for the review, just to give the auditors a sense of why the review is occurring. Also, I would encourage you to, rather than just call and say I want to review work papers, go in a room and review them, it would be better I think to engage the auditor in a dialogue about their audit approach.

Part of what this session is about and, I think, other initiatives that the OCC and the federal bank regulators have taken of late is to try to get auditors and examiners in these situations to have more clear communication on expectations and objectives. And I think that goes for work paper review as well. It helps an auditor to know the reasons why the papers are being reviewed. If they're being reviewed because generally the examiners want to make scope decisions, then that's helpful to know. If it's because there's a specific concern about a specific transaction or control

issue in an institution, it's helpful for the auditor to know that, so that if there's anything that can be helpful for the auditor to supplement orally or to discuss in that area, that appropriate communications can occur between the bank and the auditor and the examiner.

So, I would hope that the resistance that you may have experienced in the past subsides, as there's greater communication by the profession, that examiners should not be encumbered in their access to papers. And I think on your end that that could be facilitated by having a little more dialogue about purpose and then following up with the auditors at the results to give your feedback to them, so they know what the results of your review were. And I think that will go a long way to overcome any kind of resistance that might exist.

Zane Blackburn: This is Zane. I think Bill gives excellent advice. And one other thing that I might add, too, is to try to facilitate the arrangement with our examiners and the outside external auditors; we've tried to act as facilitator from that standpoint, if in fact you do encounter any type of resistance or problems. And you know, we will—I am, or any member of my staff is, certainly available to assist in that whole process. And as Bill has indicated, I think because we have tried to improve the communication and in fact been successful, that resistance and difficulties that we were seeing initially have been reduced substantially and I think they will continue to be.

Wynne Baker: Zane, this is Wynne. Let me make a comment about this. From the AICPA's perspective, in particularly from the regulatory task force, we have tried to do a job trying to educate the CPA profession on what the rules are and how important it is to work with regulators and to work with banks to try to show the work papers to them. Anybody who gets the

Journal of Accountancy, the November issue, there is an article in there quoted by several of our AICPA folks, and Mark and Zane both are quoted in there. We're trying to work together on this to make sure that the resistance is removed, because I feel that our profession has an obligation and responsibility to work with regulators and with banks to show those work papers.

William Lewis: This is Bill again. One thing I would also add, to echo the comments that actually Wynne just ended with. It really is a three-way process as well. The AICPA's standards in this area require that we make management aware of any requests for access to our work papers and that we get their consent and that they have to obviously give it under the FDICIA, but the important thing here is that the discussions between auditors and examiners under the AICPA's guidance should really involve management, or at least give management the opportunity to be involved and then, or at least know about it, and decide whether or not they want to participate. And so if you find resistance sometimes from an auditor when they get a direct communication from an examiner, in some cases it may be simply that they're obliged to have communications with their client about that request before they proceed. And that's just one thing to be aware of. And to the extent that management could be notified at the same time, again, about the nature of the review and its purpose, that, I think, would go a long way to facilitate the good coordination of the review.

Jim: Alright, just a reminder to everyone. That if you do have a question or comment to share with our panel, all you need to do is simply press one on your telephone. That brings you into the lineup here in our system. Again, I'll call on you by the city and the state and the first name of the person who registered at your site. Let's go to East Brunswick, New Jersey, and this is Ahmed's site. So East Brunswick, go ahead.

New Jersey: Hi, we have two questions here to ask you. In respect to—and anyone can answer that—in respect to the analytical procedures that were mentioned earlier, how effective can analytical procedures be in light of September 11 and the trend of interest rate adjustments both pre- and post-September 11? Does anybody want to respond to that?

Zane Blackburn: That's a hard question. Bill?

William Lewis: Yeah, I think it's a good example of why analytical procedures are not static. And what an auditor needs to do, if you look at the outline in which we describe the area surrounding analytical procedures. It's really all part of assessing the control and the inherent risk, and deciding whether or not that the assumptions used by the auditor in assessing control and inherent risk are actually validated by trends. And clearly if there is an event like September 11, then inherent risk is going to increase. And so, if I had done certain analytical procedures in the past—pre-September 11—that didn't consider a risk like that and shouldn't have because it hadn't happened, and then I have an event like September 11 that skewed credit or interest rate or other sort of risk, then I would need to tailor my analytical procedures to consider that. And that's a very good question. And actually it points up the comment that I made during my presentation, that risk assessment is not a static process. If I begin an audit, let's say of a large entity that takes say several months in July, and a major event occurs part way through, like September or October or November, I do not proceed with the tests that I designed in July and act in a way that's oblivious to that event. I need to stop and consider that or any other event in terms of the risk assessments I originally made, in terms of the audit tests I decided to perform, and then recalibrate my audit approach to deal with the risks, whether they be inherent risks for an event like that or control risks

where a company has either taken an action or something has happened to the company to change the way it either conducts its business or it monitors and controls its business.

Zane Blackburn: Go ahead with your second question.

New Jersey: Yes, definitely. And this is for the OCC. How does the OCC view having the one outsourced firm performing both an internal and an external audit function for a financial institution?

Mark O'Dell: The short answer is if you look in our *Comptroller's Handbook* booklet, our handbook discourages the same firm doing both the internal and external audit ["Internal and External Audits," July 2000; see also "Internal Control," January 2001, available on the Web at http://www.occ.treas.gov/handbook/S&S.htm]. With that said however, we recognize that presently there's no statutorial requirement that forbids that kind of arrangement, so when we do encounter it, we will look and make sure that there's the appropriate divisions and controls over from a management perspective and monitoring and controlling the outsourced audit. We will look at the outsourced audit as the responsibility of management, in that we will expect to see within the bank controls that will manage, control, and direct that outsourced activity.

Now, with the new FCC rules, there are some new ground rules. We are in the process of trying to incorporate those into the outsourcing guidance and Zane may have some further comments about that. He is at least the OCC's representative on FFIEC, that's the Federal Financial Institutions Examination Council, the interagency work group that's looking to revise the outsourcing guidance that we do have.

Zane Blackburn: Let me just mention a couple things in that particular area. Number one, although we clearly do

discourage the internal and external audit being done by the same firm, simply because I think there's a lot of benefits to having a second set of eyes, kind of a checks-and-balance perspective there. On the other hand, we're not saying that outsourcing itself is a difficulty or something that we would discourage. Rather we've actually seen a number of instances where the internal audit function has actually been improved by outsourcing it. Obviously that's on a case-by-case situation—that's circumstance-specific.

With respect to the AICPA's new independence rules, we are, as Mark has indicated, in the process of revising our statement on an interagency basis dealing with outsourcing and the independence issue in response to this. Clearly for institutions that are required to be audited that are over $500 million and are registrants of the FCC, the FCC independence rules will apply. What we're looking at now is the institutions under the $500 million mark that are not required to have audits but in fact do have audits on a voluntary basis, which we certainly do encourage. The FCC's rules provided a $200 million exemption for the internal audit outsourcing aspect of the revised independence rules. So, what we're looking at now is for those institutions between $200 million and the $500 million, whether in fact we should provide some potential relief in a hardship situation—where the bank in a particularly small area doesn't have the expertise available by a number of auditing firms, because bank auditing is very specialized and it does take very specialized individuals to audit that. So that's where our discussion lies at this point.

Mark O'Dell: Yeah, let me reiterate a point that Zane made. This is Mark again. We as an agency and I believe as the banking agencies, the FFIEC, see there are benefits in outsourcing. Particularly, smaller banks are able to use the expertise that does exist in external firms. They're able to access that expertise and

use that expertise to improve their risk management process. So, the function of outsourcing is a valid and a beneficial one to the banking industry.

Your question was, though, in terms of the same firm doing both. And that's where there's the issue of outsourcing to the same firm, the same external audit firm that does the internal audit work. There are complications that the issue of ensuring that there's appropriate separation between the two functions. So that the same department within the external audit firm or the same people do not confirm, if you will, from an external audit point of view what is being done internally.

So the issue is not outsourcing, because we do see that there are many benefits to the outsourcing function to the banking industry. It's just ensuring that there's the appropriate independence and separation between the outsourced internal audit function and the external audit function, when those two activities are being done by the same firm. Now, we may have slightly different perspectives. Maybe Bill or Wynne would like to comment on that?

William Lewis: This is Bill. I agree that, you know, that there definitely are requirements even in the AICPA's literature about extended audit services in ensuring that there are proper responsibilities taken by management in such cases. So, I note that the comments made about circumstances being different when an external auditor continues to do the work or does the work rather than an auditor that's not associated otherwise as an external auditor. There are differences and they're provided for in the AICPA literature. I think that the task force that Mark mentioned earlier that Zane is involved in is an important task force to help clarify what the regulatory expectations are, if they are different in any areas from these AICPA rules. It's important that auditors

know what those differences are. It's important that the accounting or the public accounting profession know what they are and the banks know what they are, so that they do the right thing. Also in light of the fact that the rules for public companies have changed recently. I think that task force is a good task force to try to clarify where the regulator view comes out, vis-à-vis those changes.

Zane Blackburn: Thank you, Bill. Jim, do we have another question?

Jim: Yes, we do. We have a few folks on line with us. And we have plenty of time left, so if anybody does have any questions or comments to share, simply press one on your telephone that brings you into the lineup. You can also fax in your questions, too, at 715-833-5469. So, like I said, we do have plenty of room for questions. Let's go to Berlin, Wisconsin. This is Jenny's location. So, Berlin, go ahead.

Wisconsin: Hi, my question is that going back to the questions from River Falls, I don't think you really answered it in what he was looking for. He was talking about an annual EDP audit or information technology and so forth. I think he was looking for some guidance in relation to how do we determine which accountant is giving us the best proposal, giving us the correct information for the scope of their audit, and so forth.

The reason why this is a topic for me is because of the fact that we've always had an annual EDP audit by an external firm. They used to come in for two days. It was a two-day process where they would come in and they'd look at our information systems, they would look at our policies, our procedures, our training, all of those types of things. Now when I called and asked them to send an engagement letter to do this information technology, or EDP, audit this year, they told me it's a six-month

process. They said that they are, they spent three days with the Federal Reserve Bank and that the hot topic this year, which he also asked about, is privacy issues in your information technology. So, I guess that's what I'm looking for some answers for.

Zane Blackburn: Well, let me ask. I think your question is excellent in terms of trying to get some assistance in evaluating the auditor's proposal. Assuming that you didn't get one from either Arthur Andersen or PricewaterhouseCoopers, maybe I can ask either Bill or Matt to share some views with you.

Matt Lusco: This is Matt. I would say that it sounds like you've got a fair amount of frustration about establishment of scope and potentially what has been of value to you and what is a perhaps misunderstanding or concern by your service provider, or who has been your incumbent service provider, about what may be expected from an examination standpoint. As it relates to, and I would certainly ask Zane or Mark to step in here, but it relates to examiner expectations, that's quite varied as it relates to the information systems area, and, like virtually any other area, it's going to spring from the examiner's level of confidence they've got with management's control over that area.

From a FDICIA perspective, and you didn't mention whether you are a FDICIA institution, consideration of your information processing, and control techniques embedded in that, are critical to that process, whether your service provider has a role in that or not, is another element to consider. But I think all of this frames pretty well the frustrations and concerns about not having a good dialogue among the three relative parties involved—the institution, the examiner, and the independent service provider—to really make sure that they've got an understanding of the risks that are trying to be addressed, and the scope, and the expectations. So, I would encourage you to really just to engage in a very active

discussion with your service provider and, if you're providing this report to the examiner, with the examiner as well.

Zane Blackburn: Thank you, Matt. Bill or Wynne?

Wynne Baker: Zane, this is Wynne. Let me try to address this a little bit, because we do quite a bit of this and I think the issues that you struggle with here. One, I think it's important, as Matt said, the number one thing obviously is the control environment. And I think the issue here is to have a discussion, one, with the regulators in terms of what their expectation is from a control perspective. But I think from the provider, what do you, you know, we look for somebody like us would be the issue of whether we can do the penetration test, whether we have that capability, can we assess the system, do we have the training to do that? I think the privacy is important, but I think the issue of doing samples, you know, testing accruals, all of those kinds of things over the Internet. It's important to determine whether somebody's making some money or not and I think one of the things the regulators want to look at is, obviously, the work papers that are involved. You know, there's an FFIEC policy that's involved here and certain things that have to be done. I personally don't think that that's a six-month process. Again, I think Matt asked a good question and that's whether you're over the $500 million limit or not. But I think it's important that the regulator and the bank and the provider have a discussion to understand expectations. Zane?

Zane Blackburn: Yeah, I think that's excellent advice.

Mark O'Dell: I would just moderate that slightly in that there should be, you should have a clear expectation from your discussion with your examiner what issues they see need to be addressed in the audit program. So, if you don't have those clear expectations, I would encourage you to go back to your examiner-in-charge and have whatever discussions are necessary, so that

you're really clear on if there are issues that have been brought up during the exam process that they have been clearly articulated with you. We will, and our exam staff will, be available to discuss that with you at what length each that you need to really get a clear understanding of that. I would, I don't think they would be and it's not our role to mediate or moderate between you and your vendor. So, we will provide you with clearer expectations of what we feel are the issues that need to be addressed in the audit function, again, based on your bank's size and complexity. And we will help in any way we can from that side. But, hopefully, that will give you enough information that you can then go to your vendors, and that maybe a plural, to craft and design an appropriate audit program that meets both needs.

Zane Blackburn: Thanks, Mark. Another question?

Jim: Yes. Thank you very much, caller. And we have about 10 minutes remaining in the program. We do have a faxed-in question. It comes to us from Bill in Syracuse. He would like to know, "In a small financial institution," this goes back to outsourcing internal audits by the way, "In a small financial institution, less than $200 million, who other than the audit committee should be the internal audit manager that oversees the internal audit function?"

Zane Blackburn: Let me take a stab at it, I would ask Bill and Matt and Wynne to join in as well. One of the key issues, I think, in terms of our expectations is that you in fact do have someone that's, from the bank's standpoint, that's actually taking the responsibility for the audit. As Mark had indicated, particularly in the smaller institutions, using outside expertise, I think, can be extremely beneficial, but yet it's still the bank's responsibility. I think the AICPA's ethics rules and dealing with these types of engagements recognize that that's in our existing

Interagency Outsourcing Statement. I think, in terms of, well, who should actually be the one? I think the simple answer to that is, and I'm not trying to be kind of cavalier, is one that really has the greatest skills that take on that responsibility. Bill?

William Lewis: Yeah, this is Bill. I'd agree Zane. I think that, you know, when you're in a smaller institution, you've just got a scale issue that makes this a greater issue. You know, you want to see the audit process overseen by somebody who's as objective and as detached from the day-to-day business decisions as possible. And when there's a smaller number of staff, there are fewer people, or maybe it would be difficult to find anybody who's in that position. I think therefore that it falls typically to somebody who's best suited technically to carry it out, to understand the risks, to interact with the outside service provider in scope, setting, etc.

And the other comment I'd make is that the amount of time that an audit committee member or a board member spends with relation to internal audit varies depending on this issue. I think if you have, let's say you're in a larger institution where you have someone whose only job is to oversee the outsourced audit function, they're basically the internal auditor for the group. Then they're going to rely on the judgment and objectivity of that person at a board level to perhaps just simply receive reports on results, reports on scope-setting and planning in the beginning, but not a lot of great detail on how they concluded, how they came to their decision making because they're going to rely on the judgment and objectivity of that professional. I think if you're in a situation in a smaller institution where you have an unavoidable segregation of duties issue, then I think the audit committee and the board is going to have to spend more time understanding the decisions that were taken by that individual as they governed and oversaw the

external auditor. And ask challenging questions if they feel that there's a lack of objectivity, or there's any kind of inappropriate oversight or maneuvering of that external auditor into areas that are not risky. So I think that it's just that the governance, the responsibilities on the governance at the board level, increase in that kind of an environment, vis-à-vis the amount of time they need to spend in overseeing that function.

Wynne Baker: Zane, this is Wynne. We do several outsourcing relationships for institutions under $200 million and typically what we see, and I think the first issue, is the segregation of duties, but typically what we see is somebody who is in a management role to expedite the process within the bank. And typically the second thing we see is somebody who has financial or compliance background. Maybe somebody who works for the CFO or somebody who's a controller or some type of assistant, or somebody who's got compliance background. And then the third one, sometimes there are people who have an audit background maybe working in the CFO who actually oversee that. But a lot of issues that typically would be somebody who's in a management role to facilitate the process between getting information for the outsource and then helping coordinate the meetings with the audit committee, and then making sure that findings and recommendations are expediated in terms of making sure that the audit committee, you know, has the right information to make decisions about the processes and the controls that need to be in place.

Jim: Alright, we have about five minutes remaining in the program and a couple questions yet remain in the queue as well. Let's go to Moorestown, New Jersey. This is John's location. So, Moorestown, go ahead. Moorestown, are you there? Unmute your telephone and go ahead. No? OK, we'll go on to Miami, Florida.

And I guess we won't. My goodness! Let's go on to Reston, Virginia. And this is Rodney's location. So, Reston, go ahead.

Virginia: Hi, good morning. My question is, in establishing a risk assessment matrix, is there a standard matrix that the OCC prefers a community bank or a financial institution to use? And are there any examples provided by the OCC?

Mark O'Dell: We don't have any standard risk assessment formats that we would expect to use. And that would be a question that I would ask, a discussion that you should have with your examiner. We don't have any standard form. From a policy perspective here in Washington, we have not issued any examples of risk assessment formats that we would expect to be used. The risk assessment process though, broadly speaking, is embedded in our *Comptroller's Handbook,* (our "Large Bank Supervision" [May 2001] and our "Community Bank Supervision"[August 2001] handbook booklets [available on the Web at http://www.occ.treas.gov/handbook/S&S.htm]), where that risk assessment process should include identification; it should include measuring; it should include controlling and monitoring—many of the issues that Bill brought out today. But in terms of a standard format, no we don't have one; that's something that can be tailored specifically to the issues and the risks that your particular bank assumes.

I know that's not real helpful but I would hope that as you dialogue with your examiners, as they come in, as they do their quarterly reviews, that the approach that you're taking, that you're getting good feedback on that approach. And that you have a clearer sense that if there are any regulatory perspective issues that those issues are being identified and discussed with you on a very timely basis.

Zane Blackburn: Let me just add one aspect to Mark's remarks. And that is one thing that I think that can improve the whole risk assessment process is—particularly if you have an external auditor and an internal audit function as well, if the assessment is done kind of on a joint basis—to see if in fact you do share similar views in terms of where the particular high risks are. Not that it necessarily has to be in that fashion, but I think you can benefit from each other's perspectives in those situations. Jim, do we have another question?

Jim: Yes, we do. We have just a couple minutes remaining in the program. We will go to Short Hills, New Jersey and this is Sharon's location. So, Short Hills, go ahead.

New Jersey: Hello, my name is Jim Nowe. I'm a full-time IT examiner here in the OCC for the Northeastern District. And obviously IT audit work has become a topic of this conversation. I thought I'd jump in and maybe add a little bit more granularity to the discussion. As far as the questions concerning how to work with your third-party provider in developing your IT examination scope, clearly one of the first things that the bank management and audit committee need to do is really understand the technology that they're employing in the bank and how they're used in managing information that they have. And what is the critical nature of the information that they are managing?

So obviously coordinated processing would be an area that would have significant risk associated with it. It's entirely possible that your local area, or wide area, networks might have a significant amount of risk associated with them as well. It would depend on the type of information that is being held and stored there and how that is being used. So what you would need to do is look at that from a risk perspective and design a program that addresses each of those areas of technology that do capture where

your biggest risks lie, and then present that proposal to your third party. Hopefully, what they will do is work with you, then, and provide even further granulization on the overall scope and strategy of that particular audit. The expectation is that your third party would have greater expertise than maybe the bank management would in really understanding how to address those risks and they would work in a cooperative effort in actually designing the final scope and objectives of the IT audit. The product of the IT audit we would expect would have some conclusions as to overall control. And we would like to see some sort of prioritization of what some of the key weaknesses or risk areas were defined and what recommendations are that need to be completed. So that management is focusing its resources on the more critical weaknesses as opposed to looking at everything—that may be more of a shotgun approach. So it's really important that both the bank and the third party work together and develop a sound IT audit program that really does address and assess the risks that are unique to that individual financial institution and the type of platforms and systems that they use. And anyone else is free to comment, certainly.

Zane Blackburn: Well, Jim, thank you very much. I think we are probably at the, close to the, end here. I wanted to just conclude with a couple remarks. This is actually just the first in our Audit Roundtable series. I personally want to thank each of you for your participation and excellent questions and for our speakers for their very insightful remarks. Just as kind of a reminder, there are two more parts to this series taking place this December and April of next year. And also we would appreciate very much if you would complete the evaluation form to assist us in improving those next two sessions. Jim?

Jim: Alright, thank you very much, sir. This concludes today's telephone seminar titled, "Audit Roundtable, Part 1—Risk Assessment and Internal Controls," brought to you by the Office of the Comptroller of the Currency. As a quick reminder as mentioned, please fill out and return the evaluation forms in the manner listed on those forms. Your comments and suggestions are important to us. Thanks for joining us today. Enjoy the remainder of the day. And you may hang up your telephone now. Thank you.