Written Testimony
Thomas Kimner
Risk Manager, SAS Americas' Risk Practice
September 17, 2009
Before the House Financial Services Subcommittee on
Oversight and Investigations
Hearing on "Technology to Improve TARP and Financial Oversight"

Chairman Moore, Representative Biggert, members of the Subcommittee, I appreciate the opportunity to appear before you today to speak about how technology might improve oversight. By way of background, SAS is the largest independent software analytics provider in the world, with 11,000 employees globally. We help our customers integrate data from multiple sources and, using a variety of proven analytical techniques, help them make sense of that data. By providing sophisticated tools for analyzing information, we help our customers answer three fundamental questions: what happened, why it happened, and what might happen next. To illustrate with a more concrete example, think of that telephone call you might have recently received asking to validate a particular transaction on your credit card. Analytical software such as that offered by SAS, working behind the scenes, "flagged" that transaction, either for the bank or the credit card company, as being outside your normal spending pattern.

SAS software has been used to provide data management and analytic solutions within the federal government since SAS was founded in 1976. SAS has also been working with financial institutions for more than 30 years. Currently, more than 3,100 global financial institutions use our technology to help with activities such as fraud detection, risk management, regulatory compliance, and data integration. We are recognized by independent third parties such as Chartis, IDC, and Gartner as a leader in a number of market segments, including advanced analytics, credit risk management, and operational risk management.

Given the breadth of the hearing title, there are many issues that we could discuss, but I will focus my comments on a few basic themes:

1. The role of the federal government in the financial markets is evolving. As markets become more intertwined, complex, and hurried, regulators will need to get more sophisticated to remain current with market forces and how they approach their mission.

2. The use of powerful technological tools will become increasingly important. Technology can also play a powerful role in assessing the performance of specific programs, but more can be done by both Congress and the regulators to define objectives upfront. While sophisticated tools exist, the need to effectively gather and analyze data is part of the base foundation required for oversight.

3. Risk and risk management techniques have not been universally understood. Risk management capabilities must be improved by bringing together both the "art" and the "science" necessary to effectively manage risk. Technology can bring more "science" to risk management, but there is also a need to have sound policies, practices, judgment, and accountability in place to address the "art" of effective risk management.

Complexity and Sophistication in the Regulated Environment

It probably goes without saying, but it has been a number of years since Congress last revisited the nation's financial regulatory structure. Since Gramm-Leach-Bliley was enacted, our markets have become both more global and more interrelated. We have a whole new set of financial instruments that did not exist previously. These instruments, including a variety of derivatives, Collateral Debt Obligations, Mortgage-Backed Securities etc., are highly complex and/or are based on other highly complex instruments. Our financial institutions themselves have become much more complicated, particularly as they begin to enter lines of business and sectors that they were not in previously. For example, we now have investment banks that are bank holding companies such as JP Morgan Chase, and we have traditional bank holding companies that are now in the investment banking business, such as Bank of America with its purchase of Merrill Lynch. As a result, many of these organizations are now facing regulators and regulatory objectives and compliance issues that are new to them. In addition, it is no secret to this Committee that we are seeing growing concentrations of risk in the marketplace in fewer organizations.

In short, managing these entities and their portfolios of investments and enterprises is, in this 21st century, virtually impossible without embracing technology. While it may be axiomatic that the financial sector may need more technology, regulators will also need better access to information to effectively understand what is happening in individual financial institutions and across the marketplace.

Powerful Technologies Exist to Enhance Oversight and Risk Management

At SAS, we recommend that our financial institution customers approach risk management comprehensively, by deploying tools that address market risk, credit risk, asset and liability management, and operational risk. These technological tools enable users to:

- Value instruments in their portfolios using third-party libraries or user-defined functions;
- Perform Value at Risk and stress test analysis using standard and advanced methods;
- Assess the rating of their credit portfolios and calculate advanced credit portfolio and counterparty exposure analytics, including netting, collateral, and margining;
- Perform integrated asset and liability risk management and stress testing, taking into account other risks;
- Assess firm-wide risks using economic capital, correlated aggregations, bottom-up correlated risk drivers methodology, or a combination thereof;
- Perform fair value calculations, funds transfer pricing, risk-adjusted transfer pricing and RAROC calculations;
- Perform portfolio optimizations—risk return optimization, hedge optimization and cash flow replication optimization; and
- Perform model back-testing and scenario testing of models.

These same technologies should be used by the financial regulators. These tools provide not just better insights into what is happening within a financial organization, but could provide a comprehensive assessment of that organization. And, having access to these tools will significantly advance oversight by providing a more analytic approach. The tools provide the "science", although they still require judgment to apply and analyze the resulting information.

Let me spend a few minutes highlighting a few critical technological tools that may prove valuable for oversight: stress testing, counterparty credit risk, and performance measurement.

Stress testing

Financial institutions have been doing stress testing for some time now. Traditionally, the stress tests have been conducted over single product lines—say, within a mortgage line, or credit card line. There has been limited "cross firm scenario" testing, or bringing some or all of the portfolios together to test more broadly. Because these products typically are managed individually, the "risk assumptions" may differ by product line. Changes in interest rates or unemployment rates affect these product lines differently, and need to be adjusted accordingly. This has been difficult to do historically because the process for stress testing has been, and largely still is, manual and highly labor intensive. Additionally, the regulators themselves have not typically prescribed scenarios for stress testing, but have instead worked individually with financial institutions on the stress test process.

The financial crisis has revealed several gaps and weaknesses in many organizational aspects of stress testing programs. Before the crisis, as mentioned, stress testing was performed mainly as an isolated exercise by the risk function within a bank and results where manually reported to regulators, often with each bank developing its own stress test criteria. Differing stress events and assumptions are frequently used in each model so outputs cannot be easily aggregated into a meaningful, combined result. Results of each model are reviewed independently, making comparison across risk types or assets impossible. Consolidated reporting and the infrastructure required to do so have also been limited, highlighting the need for improved reporting capacity or additional resources to support the current process.

This year, Treasury asked 19 of the country's largest banks to undergo stress testing, and established the scenarios under which the banks should test. (The program was formally called the "Supervisory Capital Assessment" Program.) The purpose for the tests was to help restore confidence in the financial markets by understanding which banks were healthy and which banks might need more support. The Supervisory Capital Assessment Program involved designing a valid and meaningful stress test, sending a regulatory letter mandating that banks perform the tests, compiling results, comparing bank submissions, adjusting values, and interpreting the findings—a process that took 3-4 months.

Without commenting on the results of the tests, there are several procedural issues worth noting. First, to comply, the financial institutions had to develop a one-time, manual process. In fact, it took many people within the banks having many conversations with the regulators to clarify what was being requested, and many hours to translate that into a model. It took the banks a substantial amount of time to develop and complete the end-to-end process, which will not be easily replicated. While the banks met the deadline, the information generated cannot be easily extended (i.e., used for other purposes, such as sensitivity analysis), automated or repeated.

Second, the stress test conditions may not have gone far enough in all cases nor covered the right factors. For example, banks were asked only to test for two primary scenarios. Other scenarios and other factors involving liquidity, cost of capital, and the economy should have probably been considered as well.

Third, the results that were transmitted to the regulators most likely were transmitted back using spreadsheets. While spreadsheets can be used to derive some limited analytical information, the regulators needed to dedicate substantial internal resources to process and analyze the results.

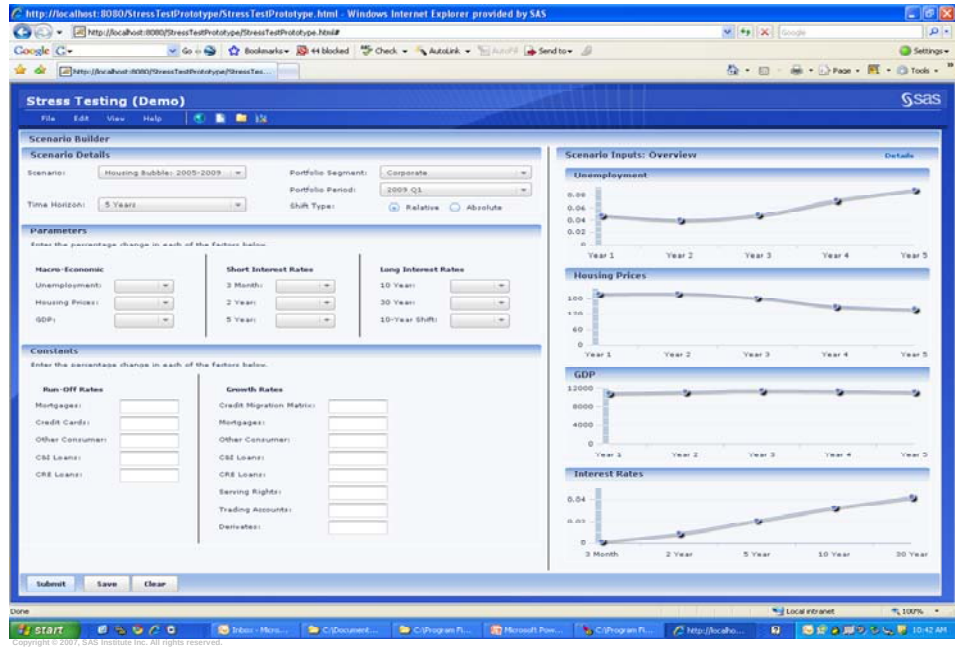
Finally, individual banks had a great deal of flexibility in interpreting and applying the stress test. There was great latitude in how instruments were treated and what types of assumptions could be made. This creates a potential issue because the perception, and perhaps the reality, is that different banks received different treatment based on varying interpretations of different results.

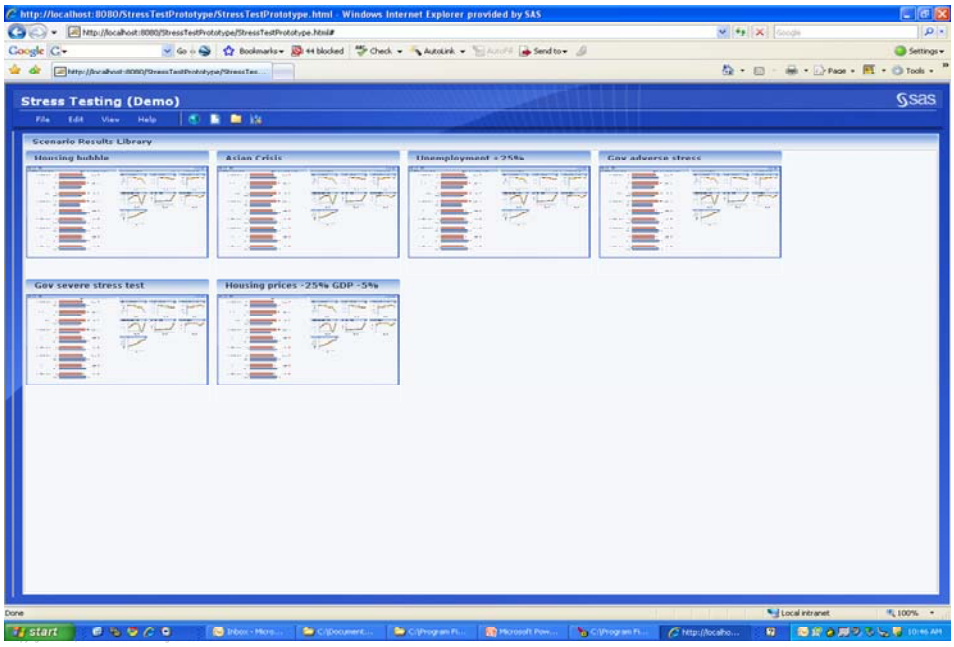
Having clear regulatory standards for stress tests and data exchange would help align asset classes and risk-measurement methodologies across the industry for use within banks, and between the banks and regulators. Setting industry standards for stress testing would help remove subjectivity from asset valuation and would provide a consistent risk calculation methodology.

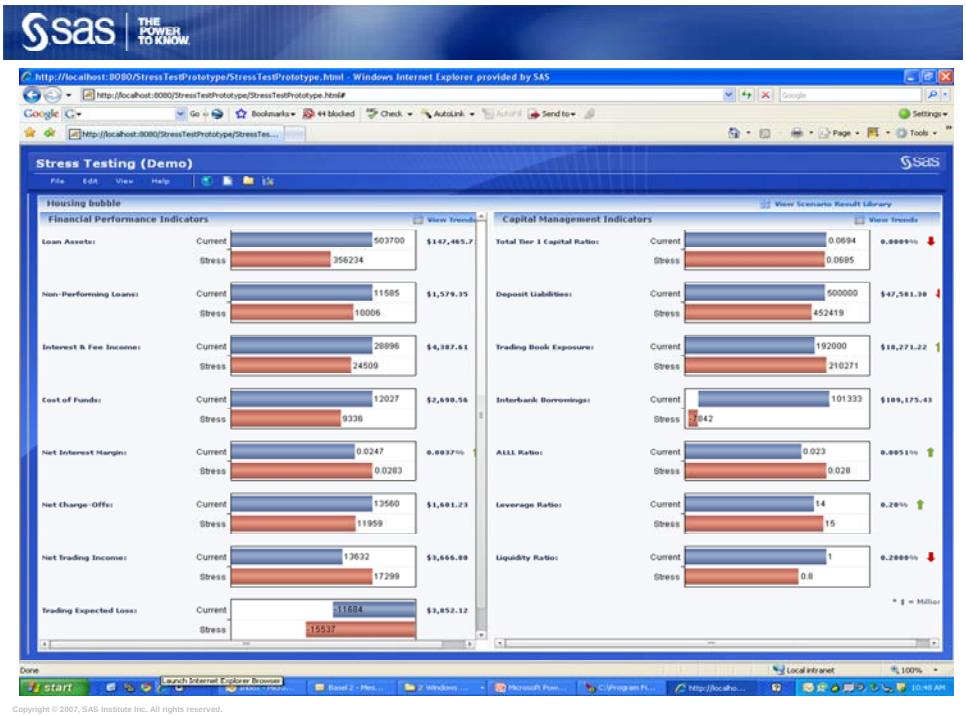
To build an effective industry-standard stress capability, coverage of all assets within banks will be needed. We can look to the Bank Call Report (FFIEC 041) as an example of standardization. This formatted report is used to collect all positions in an equivalent manner for all banks. Using the report categories as a baseline of positions establishes the universe of asset classes. Consistency is critical. Building standardized risk and valuation calculations off of the individual bank position data ensures a consistent foundation for calculations. Setting industry standards for calculations will help remove subjectivity from valuation and provide guidance for functionality.

With an increased commitment to stress testing, there is also an increased need to improve flexibility and capacity for regulatory supervision around stress testing. Establishing a standard Supervisory Capital Assessment framework would reduce valuation subjectivity. Building this capacity ahead of deep investment within each of the banks would dramatically reduce the cost of compliance, and banks as well as regulators would receive the benefits afforded from best practices and from access to shared research, expertise, and learning. In fact, we expect there will be additional stress tests, and other factors considered. Unless the banks invest in additional technology to automate the process, such future requests will again be one-off exercises that could be quite debilitating to the banks, and of marginal relevance to the regulators. But, the issue is not simply to automate the process from the banks' perspective: the regulators need the same sort of analytical tools to better analyze the information they are receiving.

As mentioned previously, technology can be of enormous assistance to both the banks and the regulators in this process. Stress testing software gives financial institutions the capability to bring together millions of instruments, the ability to stress across product lines, and to adjust for different econometric and market factors as appropriate. As important, it gives the banks the ability to objectively replicate their results, and have confidence that their results are consistent and accurate. Such software has the ability to produce meaningful information such as illustrated in the following inserts:







Counterparty Credit Risk

As you know, counterparty risk is the risk that another party to a transaction will default. How well one can "hedge" against the risk, in part, depends on the transparency of the other party. Consequently, there are those who assert that one of the issues with credit default swaps was the complete lack of transparency as to who the other parties to the transaction were, and thus no meaningful assessment as to risk could be made. Any time the government lends or guarantees funding, it encounters counterparty credit risk. Investors, for example, by investing in MBS pools or complex securities, take on counterparty credit risk. To illustrate, the Pension Benefit Guarantee Corporation takes on, albeit involuntarily, counterparty credit risk when it guarantees a pension plan.

Many of these investments come with credit ratings assigned to them by credit ratings agencies. Like private investors, government "investors" have, in the past, taken these ratings at face value, without attempting to examine the assumptions underlying the ratings. For example, certain AAA rated investments may well have had loans in the investment pool with a 50 percent probability of default. However, it is most likely that an investor in such a pool looked at the AAA rating assigned, without exploring the underlying probabilities of default. If they had, they may have concluded that such an investment was something less than AAA rated.

In developing the ratings, the agencies had to analyze a set of information. The issue for many investors, whether private or governmental, is that they have not historically conducted their own analysis of that data. Technology gives investors the ability to run independent analyses to test underlying assumptions and make their own conclusions regarding the risk presented by the transaction. From a regulatory perspective, having similar technologies enables each regulatory body to not only independently validate the status of investments, but to make better decisions about the level of capital that needs to be reserved or withheld in light of the independent risk assessment. It is a fairly simple matter to encourage any governmental body that makes loans or guarantees to have

similar technology. Running the independent analyses, however, will require some type of information that ranks or rates the potential exposure of investment and counterparties.

Performance Management

One advanced capability of growing importance is performance management. For SAS, performance management is the process of using technology to ensure that a project's goals and objectives are fully aligned with the resources and activities needed to achieve those goals. In other words, it is necessary to understand the cause and effect relationships between the strategy, activities, and resources of a project. Software tools can help project managers and senior officials within an agency understand whether the right activities are being pursued with the right resources to obtain stated objectives. Conversely, technology can highlight activities that are not useful or resources not contributing to successful completion so that decision makers can modify or even terminate the project. More important, software can help managers begin to run "what if" scenarios. For example, what happens if a disaster relief agency dedicates more people to grants management? Does that, in fact, contribute to improved grants management, and at what overall cost to the organization? Or, what is the impact on the mortgage market of injecting billions of dollars into the financial sector? How can you measure that effectiveness, or understand which activities are meaningfully contributing? Performance management software provides immediate answers to these questions and provides insight into those actions and resources that have a causal and critical relationship to the overall mission. It also provides the Administrative branch with the ability to answer oversight questions, and to do so quickly and rationally.

The challenge that we see, and see increasingly with many of the "stability" initiatives that have been undertaken in the last year, is a lack of clarity or delineation as to what the programs are actually trying to accomplish. TARP has added challenges because the objectives and activities have changed over time, and have changed dramatically from what was contemplated in the original Emergency Economic Stabilization Act. Without a clear understanding of the problem, or the objectives, or even the goals, it is virtually impossible to assess whether the activities have been effective or resources used wisely; the application of technology is no substitute for clarity. Even with clear goals, Congress needs to start asking the questions: "has this project been effective?" or, "are we measuring the right things, given what our explicit objectives were?" Performance management software will give any regulator the ability to answer those questions objectively. And, it should give Congress more confidence in the answers it receives to its tough oversight questions.

The Importance of Data

Software tools and technologies, while highly useful and necessary for effective risk management and oversight, have a significant dependency on data – both its availability and its accuracy. Effective data integration and information management are critical elements to building a solid regulatory foundation that enables agencies to draw appropriate conclusions about risk. To this point, let me set out the following scenario:

> Scores of people wrote to the SEC using many different mechanisms, raising questions about the potential that Bernie Madoff was not operating a legitimate trading operation. Many people, in many different offices and locations of the SEC, had bits and pieces of information and tips about the scheme, yet no one was able to put the entire scheme together until it was much too late.

I raise this scenario to make several points. The first is that the financial regulatory agencies have data. In fact, they are probably drowning in data. The issue is what to do with that data. In the SEC scenario, decision makers were not able to put all the data together to get an accurate picture of what was

occurring. Without a single and consistent view of what is occurring within an organization, no financial regulator will be able to fully understand the challenges and problems that it may be confronting. Without that complete understanding, there is no way a regulator is going to make an informed decision as to the best actions to take under the circumstances.

By using data integration technologies, an agency's internal information sharing capabilities can be improved. These technologies are equally important at improving the information sharing abilities between and among federal financial regulators. Without better means of sharing information among the regulatory community, the actual results of the regulatory structure will probably not meet expectations. Solving the technological issue of how to share data is the easy part of the question. The harder parts involve convincing regulators to overcome territorial concerns. Technology can help ease some of these issues through things such as audit trails. These audit trails can show who accessed the data, when, and how it might have been altered. However, technology cannot resolve the cultural issues that prevent or discourage information sharing among divisions or among agencies. Those cultural boundaries have to be broken by dedicated, outspoken leadership from the regulatory organizations. We are encouraged, for example, by the recent "harmonization roundtables" held by the CFTC and the SEC, but other efforts will be needed.

Data gathering and integration are thus foundational technology steps. Once the appropriate data is integrated, the agencies can then apply advanced analytical capabilities to understand what is important from that data. Advanced analytics provide insights into trends and patterns, and can be applied to provide information in seconds, not days, weeks, or even the months that it can often take some regulators to generate information. In the SEC example, analytics could have been applied to validate or debunk alleged trading patterns or to discern potential frauds.

Risk Management is both Art and Science

Risk, quite simply, is the uncertainty of an outcome. Dedicated risk management, a growing corporate practice, is proactively managing for the uncertainty. For financial institutions, risk management is determining what level of risk an institution is willing to absorb, and then managing the business (e.g., selecting which investments to make, which assets or liabilities to purchase, what procedures and policies should be put in place) according to that risk tolerance. On a macro level, risk management should involve a review as to whether individual financial institutions are adhering to their own frameworks, as well as making decisions regarding what is an acceptable amount of risk in the marketplace as a whole. For SAS, good risk management is about providing a framework and technologies to be able to manage the exposure based on risk criteria that an individual bank deems appropriate for itself. Regulators should have similar capabilities to make independent assessments of the risk exposure of that bank and all banks given their charter to protect entire market.

In many companies, a dedicated risk management function is a fairly recent development for US financial institutions. As such, there is wide divergence among institutions as to what constitutes good risk management. Historically, regulators have approached their job as applying a checklist of conditions to their regulated entities, with little real understanding of what constitutes relevant risk management—what one might call a "rubber stamp" approach. It is often perceived that if the institutions could show they had certain minimum techniques in place, they were credited with having "risk management" practices. There was little required to prove that the practices were appropriate for the activities and actual risks being undertaken or that they were even well-understood by those undertaking them. Stated another way, there was little in the way of due diligence or otherwise trying to ascertain what was behind the numbers. Similarly, there is very little consistency among organizations, or standard inputs. We submit that historically, regulatory oversight was more art than science, perhaps performed by those not always fully qualified to assess risk strategies. We are not

suggesting everyone should use SAS' models or technology, but rather, that there should be a common understanding within the industry about the kinds of actions that should be considered.

Let me set out a second scenario:

> In recent years, US financial regulators relaxed U.S. capital rules. In doing so, many companies that now no longer exist (Bear Stearns, Lehman Brothers to name two), had leverage ratios of 33 to 1. In some cases, debts were 60 times the amount of assets. By contrast, Canadian banking regulators set leverage ratios at 20 to 1, with the result that Canadian banks have fared better than their US counterparts. US regulators were not able to accurately predict the effect of their policies. Had they had the right technology in place, they could have tested for various scenarios in which the 60 to 1 debt ratio would have been shown to be a distinct possibility. With that insight, regulators would have been in a position to adjust or modify policy proposals to ameliorate some of the more extreme potential consequences.

Technology, if utilized properly, could have revealed the potential consequences of changing regulatory requirements. However, part of the issue is whether proper judgment was used in making the changes. As such, while technology, or "science" can provide insights, it needs to be combined with judgment to have the best effect in risk management.

We draw several other observations from our experience. First, it is crucial that we develop a common framework for what is good risk management. By this we do not mean to prescribe the exact practices or precise "risk appetites" that financial institutions should undertake or have. Rather, we mean that given a set of risk appetites, what acceptable regulatory practices should be in place to mitigate those risks. Under this scenario, and assuming all banks had equally strong policies and procedures in place, banks engaged in less risky behavior would need less rigorous controls in place because their exposure to uncertainty from their financial investments is less. On the other hand, those "cowboys and gunslingers" that have a larger appetite for riskier transactions would need more vigilant risk controls.

Second, all entities need to do a better job analyzing the risk inherent in each and every transaction, in each portfolio, line of business, and business unit. These analyses need to be applied across the entire enterprise and not just in individual business units. This will help account for concentration risks and exposures that are crossed and/or embedded in different areas, which may extend beyond individual business unit tolerances or limits. Applying integrated technology across an organization, or even across organizations, can easily help to identify these limits and set alerts when these limits are reached or exceeded. The technology acts much like a thermostat on the nation's economic health.

We are beginning to see the regulators move away from the historical "rubber stamp" approach, to undertaking more due diligence and improving transparency. These efforts are taking the form of having regulators and auditors actually look at procedures and policies in place and asking tough questions about whether such policies and procedures are being followed and how consistently. This is a positive development, and a direction that should be encouraged.

Final Thoughts

SAS' catch phrase is "The Power to Know." We believe that data and the types of technological tools described above, if properly used, are powerful enablers. They allow decision makers to draw mathematically significant insights about their actions and, consequently, to make better, informed decisions. As decision makers, regulators—whether financial or oriented to other sectors—would equally benefit from analytical solutions such as those SAS provides. And, as our markets and financial products become increasingly complicated and interrelated, technology must be incorporated to assist in understanding and monitoring what is happening.

Technology, by itself, is not sufficient for sound risk management or proper regulatory oversight. Policies and procedures are a critical leg of this "three-legged" stool. There are many policy questions, which include:

- What policies are in place regarding the credit space?
- What policies are in place to ensure that sound underwriting practices are being followed?
- What types of concentrations in individual and geographic markets are developing?
- Are there policies and procedures in place regarding decision and commitment authority, reflecting concerns that no individual be allowed to over commit any individual financial institution (a lesson that was learned the hard way in Bearings Bank)?
- Are there appropriate audit, accountability and governance practices in place?

These are the types of questions that regulators should be asking and have begun to ask.

What might be receiving the least amount of attention is whether our regulators have sufficient resources and people in place to conduct good financial oversight. To understand the technology products, the information they produce, and to correctly interpret the results of audits or investigations requires specific skills and knowledge. Pockets of analytical expertise currently exist in the government, but these pockets are spread thin. We are concerned that our federal workforce is aging and fewer people are deciding to enter into public service. Who, then, will have the requisite knowledge and expertise to use these highly sophisticated resources or to make sense of them? In short, technology can unlock vital insights. But whether these insights are understood or acted upon depends on the acumen and expertise of those reviewing the results. Without the right people possessing the right skills in the right jobs, technology will not provide improvements in oversight.

We appreciate the opportunity appear before you today and look forward to your questions.