Supervisory Insights

Inside

FDIC

Supervisory Insights

Supervisory Insights is published by the Division of Supervision and Consumer Protection of the Federal Deposit Insurance Corporation to promote sound principles and best practices for bank supervision.

Donald E. Powell
Chairman

Christopher J. Spoth
Acting Director, Division of Supervision and Consumer Protection

Steven D. Fritts
Executive Editor

Journal Executive Board

Donna J. Gambrell, Deputy Director
John M. Lane, Deputy Director
William A. Stark, Acting Deputy Director
John F. Carter, Regional Director
Doreen R. Eberley, Acting Regional Director
Stan R. Ivie, Regional Director
James D. LaPierre, Regional Director
Scott M. Polakoff, Regional Director
Mark S. Schmidt, Regional Director

Journal Staff

Kim E. Lowry
Managing Editor

Brett A. McCallister
Financial Writer

April G. Schwab
Financial Writer

Supervisory Insights is available online by visiting the FDIC's website at www.fdic.gov. To provide comments or suggestions for future articles or to request permission to reprint individual articles, send an e-mail to SupervisoryJournal@fdic.gov. To request print copies, send an e-mail to publicinfo@fdic.gov.

The views expressed in *Supervisory Insights* are those of the authors and do not necessarily reflect official positions of the Federal Deposit Insurance Corporation. In particular, articles should not be construed as definitive regulatory or supervisory guidance. Some of the information used in the preparation of this publication was obtained from publicly available sources that are considered reliable. However, the use of this information does not constitute an endorsement of its accuracy by the Federal Deposit Insurance Corporation.

Issue at a Glance

Vol. 2, Issue 2 Winter 2005

Articles

Regular Features

Letter from the Director

Ask any banker his view on the Basel II rulemaking and you are likely to hear conflicting responses. Given the major changes that will occur in how we measure risk-based capital adequacy at the largest, most sophisticated insured financial institutions, we should anticipate that other banks will scrutinize all aspects of the regulators' implementation plans. Many comments, including some criticism, have already been delivered by banks that will not be required to adopt Basel II. Why would these bankers take issue with the Basel II text? The most often cited reason is the potential for competitive inequity.

The results of the most recent capital impact study (the fourth Quantitative Impact Study – QIS-4) show Basel II would most likely lead to an unacceptably large decline in capital for the largest banks unless modifications are made (see the *Capital and Accounting News* feature on page 27 for greater detail on the QIS-4 results). Competing head to head with large banks, holding in some cases a fraction of the capital non-Basel II banks hold on the same loan portfolio, would be a daunting challenge for the nation's community banks.

At this point, the bank regulatory agencies have two alternatives. The first is to modify the Basel II framework to prevent substantial declines in capital — something the agencies are committed to doing should the QIS-4 results become a reality when Basel II is implemented. The second alternative is to modify the existing capital framework for non-Basel II banks to reduce, among other things, competitive inequities. This Letter focuses on the modification of the existing capital framework for non-Basel II banks.

To better understand the competitive issues Basel II may pose to non-Basel II banks, the agencies began a formal rulemaking dialogue with the banking industry. We did this with the publication of an Advance Notice of Proposed Rulemaking (ANPR) outlining potential changes to the existing risk-based capital regulations. The ANPR was unanimously approved by the FDIC Board of Directors on October 6, 2005, and published in the ***Federal Register*** on October 20, 2005.[1] The agencies are accepting public comment through January 18, 2006, and welcome a discussion with the industry, policymakers and the public.

The FDIC believes changes to the existing risk-based capital framework are necessary in order to address concerns about competitive equity, as well as many of the concerns about the risk-based capital framework generally. The proposals in the ANPR, commonly referred to as Basel 1A, are designed to be the first step toward modernizing the risk-based capital framework to ensure it remains a reliable measure of the risk, as well as minimize potentially material differences in capital requirements likely to emerge once Basel II is implemented by the largest banks.

One key proposal set forth in the ANPR addresses modifications to the existing capital requirements on residential mortgages. It is generally accepted by the bank regulatory community that Basel II banks will recognize substantial capital reductions on their residential mortgage portfolio. For non-Basel II banks, the ANPR suggests basing the risk weights for mortgages on loan-to-value ratios, a simple and straightforward measure of risk. For prudently underwritten mortgages with a loan-to-value ratio of 80 percent, the ANPR considers reducing

[1] This proposal is available at www.fdic.gov/news/news/press/2005/pr10505.html. Also see *Federal Register:* October 20, 2005 (Volume 70, Number 202), Page 61068-61078.

the risk weight from 50 percent to 35 percent. Mortgages with even lower loan-to-value ratios could have risk weights as low as 20 percent. The residential mortgage proposal shows willingness by the regulators to address concerns raised by community banks. In fact, this proposal is based largely on suggestions made by several of our FDIC-supervised banks.

The ANPR includes other specific proposals, such as increasing the number of risk-weight categories from five to nine, expanding the use of external credit rates, and widening the range of collateral and guarantors that may qualify an exposure for a lower risk weight. Such proposals are intended to encourage community banks to consider using risk mitigating techniques that lower their overall credit risk profile. In other areas, the ANPR is more open-ended, discussing concepts for promoting greater risk sensitivity in other business lines where risk measurement factors are not well defined or universally applied, such as with unrated commercial loans and certain retail loans.

In addition, the ANPR proposes modifications to the existing risk-based capital rules where quantitative factors used to measure the risk associated with a given product or exposure can be readily articulated. Examples of these changes include modifying the credit conversion factors for various commitments, including those with an original maturity of less than one year; increasing the risk weight of certain loans 90 days or more past due or in non-accrual status; and increasing the risk sensitivity of commercial real estate, retail, multifamily, small business, and commercial exposures.

While developing a more risk sensitive framework is important from a competitive equity perspective, the agencies want to ensure the burden generated by our proposals is commensurate with the benefit. In this respect, we believe most, if not all, of the proposals discussed in the ANPR could be applied using readily available information. However, we have asked for comment on whether the trade-off of a more risk-sensitive capital framework is justified by the amount of any additional burden that may be generated by its implementation. To prevent undue burden, we are looking for ways to make the application of any new capital rules more flexible. In addition, we are asking for comments on whether some community banks should be allowed to maintain "status quo" and opt out of any new framework altogether. Community banks operating with capital ratios well in excess of their minimums may suggest that we pursue this "status quo" option.

The FDIC is encouraging careful consideration of the implications of the proposals included in the ANPR. In addition to comments on the specific proposals set forth in the ANPR, we would welcome any alternatives or suggestions that will promote the development of more comprehensive proposals. Examiners should keep informed as the Basel 1A and Basel II approaches develop. ***Supervisory Insights*** is one source of information, and this issue's *Capital and Accounting News* column discusses the results of the most recent Basel II quantitative impact study (QIS-4).

Christopher J. Spoth
Acting Director, Division of Supervision and Consumer Protection

Model Governance

Financial modeling is increasingly important to the banking industry, with almost every institution now using models for some purpose. Although the use of models as a management tool is a significant advance for the industry, the models themselves represent a new source of risk — the potential for model output to incorrectly inform management decisions.

Although modeling necessarily involves the opportunity for error, strong governance procedures can help minimize model risk by

- Providing reasonable assurance the model is operating as intended;
- Contributing to ongoing model improvement to maintain effectiveness; and
- Promoting better management understanding of the limitations and potential weaknesses of a model.

This article briefly discusses the use of models in banking and describes a conceptual framework for model governance. In addition, the article suggests possible areas of examiner review when evaluating the adequacy of an institution's model oversight, controls and validation practices.

Use of Models in the Banking Industry

Fundamentally, financial models describe business activity, predicting future or otherwise unknown aspects of that activity. Models can serve many purposes for insured financial institutions, such as informing decision making, measuring risk, and estimating asset values. Some examples:

- Credit scoring models *inform decision making,* providing predictive information on the potential for default or delinquency used in the loan approval process and risk pricing
- Interest rate risk models *measure risk,* monitoring earnings exposure to a range of potential changes in rates and market conditions
- Derivatives pricing models *estimate asset value,* providing a methodology for determining the value of new or complex products for which market observations are not readily available

In addition, models play a direct role in determining regulatory capital requirements at many of the nation's largest and most complex banking organizations. Some of these institutions already use value-at-risk models to determine regulatory capital held for market risk exposure.[1] At institutions adopting the Basel II capital standards when finalized, financial models will have a much expanded role in establishing regulatory capital held for all risk types.

Not all models involve complex mathematical techniques or require detailed computer programming code. This does not, however, diminish their potential importance to the organization. For example, many banks use spreadsheets that capture historical performance, current portfolio composition, and external factors to calculate an appropriate range for the allowance for loan and lease losses. Although at first glance this may not appear to be a "model," the output from such spreadsheets directly contributes to preparation of the institution's reported financial statements, and some controls are necessary, given the seriousness of any potential errors.

Model Governance

Institutions design and implement procedures to help ensure models achieve their intended purpose. The

[1] Institutions with $1 billion or more in trading assets are subject to the 1996 Market Risk Amendment to risk-based capital regulations.

necessary rigor of procedures is specific to each model. An institution's use of and reliance on a model determines its importance and, in turn, establishes the level of controls and validation needed for that model. For some simple spreadsheet models, controls and validation may consist of a brief operational procedures document; password protection on the electronic file; and periodic review by internal audit for accuracy of the data feeds, formulas, and output reporting. While procedures will vary, certain core model governance principles typically will apply at all institutions (see Figure 1):

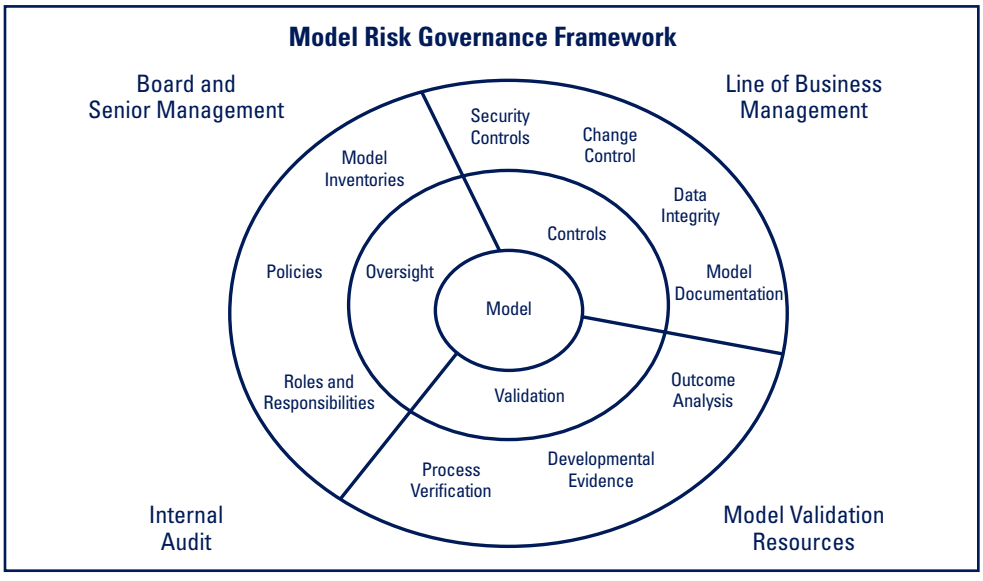
- The board establishes policies providing oversight throughout the organization commensurate with overall reliance on models.
- Business line management[2] provides adequate controls over each model's use, based on the criticality and complexity of the model.
- Bank staff or external parties with appropriate independence and expertise periodically validate that the model is working as intended.
- Internal audit tests model control practices and model validation procedures to ensure compliance with established policies and procedures.

Supervisory Review of Models

With the industry's growing reliance on financial modeling, regulators are devoting additional attention to model governance.[3] Examiners do not typically review controls and validation for all models, but instead select specific models in connection with the supervisory review of business activities where model use is vital or increasing.

The evaluation of model use and governance often becomes critical to the regulatory assessment of risk in the reviewed activities. For example, many

Figure 1



[2] Providing for appropriate controls may be the responsibility of senior management at smaller organizations.

[3] OCC Bulletin 2000-16, "Risk Modeling," (May 30, 2000) is the primary source for formal regulatory guidance on model governance available at www.occ.treas.gov/occ_current.htm.

continued from pg. 5

banks have completely integrated the use of credit scoring models into their retail and small business lending. Model results play a significant role in underwriting, contributing to the decisions to make loans and price loans for credit risk. Model results also typically are used to assign credit risk grades to loans, providing vital information used in risk management and the determination of the allowance for loan and lease losses. Therefore, examiner assessment of credit risk and credit risk management at banks that use integrated credit scoring models requires a thorough evaluation of the use and reliability of the scoring models.

Although the supervisory review of model use and governance may sometimes require quantitative or information technology specialists for some complex models, examiners can perform most model reviews. Even when specialists are used, model review does not occur in isolation; the specialist's evaluation of mathematical theories or program coding is integrated into the examiner's assessment of model use. Regulatory review typically focuses on the core components of the bank's governance practices by evaluating model oversight, examining model controls, and reviewing model validation (see Figure 2). Such reviews also would consider findings of the bank's internal audit staff relative to these areas.

Model Oversight

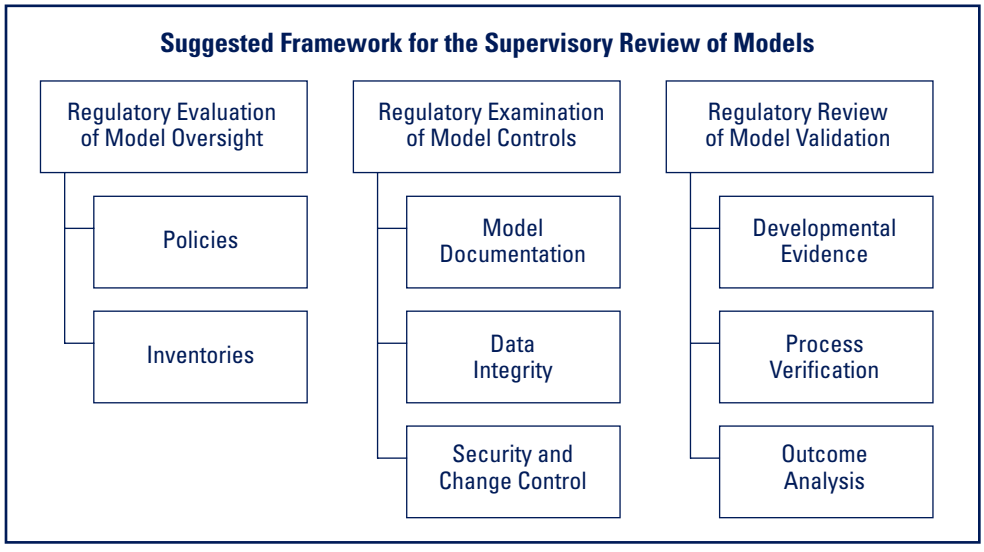
When evaluating board and senior management oversight, examiners typically

- Review model governance policies to determine (1) if the policies are adequate for the bank's level of model use and control, and (2) if validation procedures used for individual models comply with established policies; and
- Review the bank's model inventory for accuracy and completeness.

Model policies: A single board-approved policy governing models may suffice for many banks, although those with greater reliance on financial modeling may supplement the board-approved policy with more detailed policies for each line of business. Such policies typically

- Define a model, identifying what components of management information systems are considered subject to model governance procedures;

Figure 2



- Establish standards for controls and validation, either enterprise-wide minimum standards or, alternatively, varying levels of expected controls and validation based on model criticality and complexity;
- Normally require verification of control procedures and independent validation of model effectiveness before a model is implemented;[4] and
- Generally define the roles of management, business line staff, internal audit, information technology staff, and other personnel relative to model development and acquisition, use, controls, and validation responsibilities.

Model inventories: Banks of any size or complexity benefit from maintaining an inventory of all models used. The inventory should catalogue each model and describe the model's purpose, identify the business line responsible for the model, indicate the criticality and complexity of the model and the status of the model's validation, and summarize major concerns identified by validation procedures or internal audit review. Periodic management attestation to the accuracy and completeness of the model inventory is a strong practice to help ensure that the inventory is appropriately maintained.

Model Control Practices

When examining controls around individual models, regulators

- Review model documentation for (1) discussion of model theory, with particular attention to model limitations and potential weaknesses, and (2) operating procedures;
- Review data reconciliation procedures and business line analysis of model results; and
- Evaluate security and change control procedures.

By conducting their own review of model documentation and controls, examiners gain a stronger understanding of the model's process flow. This understanding enables examiners to test the findings of the bank's validation and internal audit review against their own observations.

Model documentation: Documentation provides a thorough understanding of how the model works (model theory) and allows a new user to assume responsibility for the model's use (operational procedures). Each model should have appropriate documentation to accomplish these two objectives, with the level of documentation determined by the model's use and complexity. Generally, elements of documentation include:

- A description of model purpose and design.
- Model theory, including the logic behind the model and sensitivity to key drivers and assumptions.
- Data needs.
- Detailed operating procedures.
- Security and change control procedures.
- Validation plans and findings of validations performed.

[4] Banks may sometimes face compelling business reasons to use models prior to completion of these tasks. For example, trading of certain complex derivative products often relies on rapidly evolving valuation models. Management may, in some instances, decide the potential return from such activities justifies the additional risk accepted through the use of a model that has not been validated. In such cases, management should
- Specifically approve the temporary use of an unvalidated model for the product.
- Formalize plans for a thorough validation of the model, including a specific time frame for completion.
- Establish limits on risk exposures, such as limiting the volume of trades that are permitted before validation is completed.

Model Governance

continued from pg. 7

Data integrity: Maintaining data integrity is vital to model performance. Much of the information used in a model is electronically extracted or manually input from source systems; either approach provides opportunity for error. Business line management is responsible for the regular reconciliation of source system information with model data to ensure accuracy and completeness.[5]

Data inputs need to be sufficient to provide the level of data consistency and granularity necessary for the model to function as designed. Data lacking sufficient granularity, such as product- or portfolio-level information, may be inadequate for models that use drivers and assumptions associated with transaction-level data. For example, the robustness of an interest rate risk model designed to use individual security-level prepayment estimates could be compromised by the use of an average prepayment speed for aggregate mortgage-backed securities held in the investment portfolio.

Security and change control: Key financial models should be subject to the same controls as those used for other vital bank software. Security controls help protect software from unauthorized use or alteration and from technological disruptions. Change control helps maintain model functionality and reliability as ongoing enhancements occur.

Some level of security control is generally appropriate for all financial models. Security controls limit access to the program to authorized users and appropriate information technology personnel. Control can be maintained by limiting physical or electronic access to the computer or server where the program resides and by password protection. The institution should have backup procedures to recover important modeling programs in the event of technological disruption.

Change control may be necessary only for complex models. Such procedures are used to ensure all changes are justified, properly approved, documented, and verified[6] for accuracy. Events covered by such procedures include the addition of new data inputs, changes in the method of data extraction from source systems, modifications to formulas or assumptions, and changes in the use of the model output. Typically, proposed changes are submitted for approval by business line management before any alterations to the model are initiated. To maintain up-to-date documentation, staff may log all changes made to the model, including the date of the change, a description of the change, initiating personnel, approving personnel, and verification.

When model importance and complexity are high, management may choose to run parallel models — prechange and postchange. Doing so will assist in determining the model's sensitivity to the changes. Changes significantly affecting model output, as measured by such sensitivity analysis, may trigger the need for accelerated validation.

[5] For example, the regular verification of data integrity for a value-at-risk model likely would include the following:

- Reconciliation of trading account exposures in source information systems with model inputs to ensure that all trading positions are being captured and accurately incorporated into the model.
- Reconciliation of model outputs with model inputs to ensure all data inputs are being appropriately used, with particular attention to handling missing, incomplete, or erroneous data fields that serve as risk drivers in the computation of value-at-risk for each trading position.

[6] Optimally, all changes to models should be verified by another party to ensure the changes were made accurately and within the guidelines of the approval. This does not constitute validation, but merely verification that approved changes were made correctly.

Model Validation

Validation should not be thought of as a purely mathematical exercise performed by quantitative specialists. It encompasses any activity that assesses how effectively a model is operating. Validation procedures focus not only on confirming the appropriateness of model theory and accuracy of program code, but also test the integrity of model inputs, outputs, and reporting.

Validation is typically completed before a model is put into use and also on an ongoing basis to ensure the model *continues* to perform as intended. The frequency of planned validation will depend on the use of the model and its importance to the organization. The need for updated validation could be triggered earlier than planned by substantive changes to the model, to the data, or to the theory supporting model logic.

Examiners do not validate bank models; validation is the responsibility of the bank. However, examiners do test the effectiveness of the bank's validation function by selectively reviewing various aspects of validation work performed on individual models.[7] When reviewing validation, examiners

- Evaluate the scope of validation work performed;
- Review the report summarizing validation findings and any additional work papers needed to understand findings;
- Evaluate management's response to the report summarizing the findings, including remediation plans and time frames; and
- Assess the qualifications of staff or vendors performing the validation.

This process is analogous to regulatory review of bank lending. When looking at loan files, examiners do not usually rely exclusively on the review work performed by loan officers and loan review staff, but also look at original financial statements and other documents to verify the loan was properly underwritten and risk graded. Similarly, examiners review developmental evidence, verify processes, and analyze model output not to validate the model, but to assess the adequacy of the bank's ongoing validation (see Figure 3).

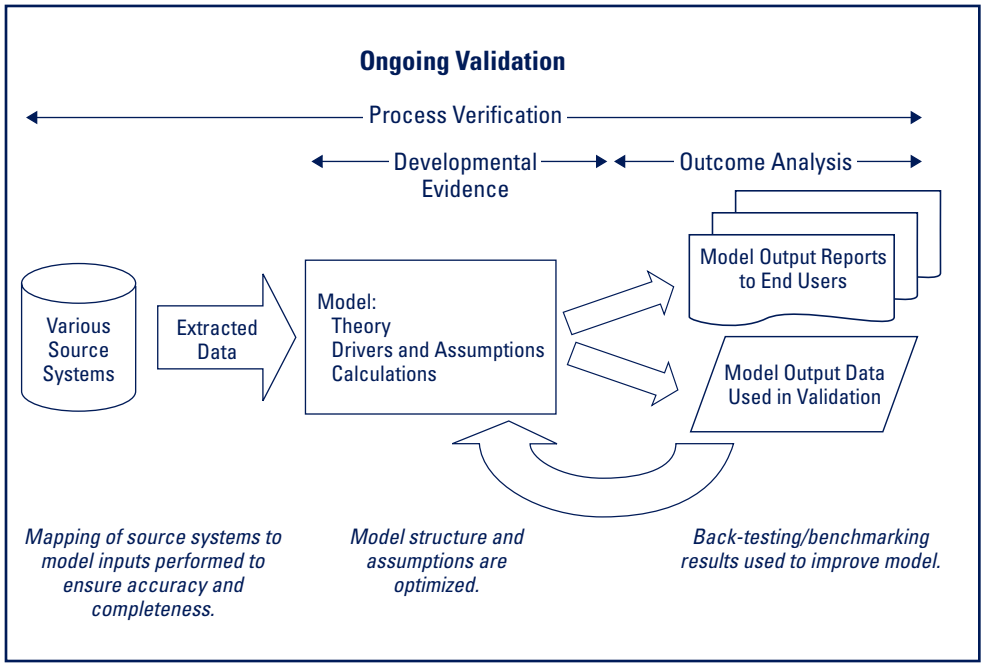
Components of Validation:

- *Developmental evidence:* The review of developmental evidence focuses on the reasonableness of the conceptual approach and quantification techniques of the model itself. This review typically considers the following:
  - Documentation and support for the appropriateness of the logic and specific risk quantification techniques used in the model.
  - Testing of model sensitivity to key assumptions and data inputs used.
  - Support for the reasonableness and validity of model results.
  - Support for the robustness of scenarios used for stress testing, when stress testing is performed.
- *Process verification:* Process verification considers data inputs, the workings of the model itself, and model output reporting. It includes an evaluation of controls, the reconciliation of source data systems with model inputs, accuracy of program coding, and the usefulness and accuracy of model outputs and reporting. Such verification also may include benchmarking of model processes against industry practices for similar models.
- *Outcome analysis:* Outcome analysis focuses on model output and reporting to assess the predictiveness of the model. It may include both qualitative and quantitative techniques:
  - Qualitative reasonableness checks consider whether the model is

[7] This review may require the use of quantitative specialists, depending on the complexity of the model.

continued from pg. 9

Figure 3



generally producing expected results.

- Back-testing is a direct comparison of predicted results to observed actual results.
- Benchmarking of model output compares predicted results generated by the model being validated with predicted results from other models or sources.

Expertise and independence of model staff: The criticality and complexity of a model determine the level of expertise and independence necessary for validation staff, as well as the scope and frequency of validations. The more vital or complex the model, the greater the need for frequent and detailed validations performed by independent, expert staff.

The complexity of some models may require validation staff to have specialized quantitative skills and knowledge. The extent of computer programming in the model design may require specialized technological knowledge and skills as well.

Optimally, validation work is performed by parties completely independent from the model's design and use. They may be an independent model validation group within the bank, internal audit, staff with model expertise from other areas of the bank, or an external vendor. However, for some models with limited importance, achieving complete independence while maintaining adequate expertise may not always be practical or necessary. In such cases, however, management and internal audit should pay particular attention to the appropriateness of scope and procedures.

Validation work can incorporate combinations of model expertise and skill levels. For example, management may rely on the bank's own internal audit staff to verify the integrity of data inputs, adequacy of model controls, and appropriateness of model output reporting, while using an outside vendor with model expertise to validate a model's theory and code.

Third-party validation: Vendors are sometimes used to meet the need for a high level of independence and

expertise. They can bring a broad perspective from their work at other financial institutions, providing a useful source for theory and process benchmarking. When using external sources to validate models, appropriate bank personnel should determine that vendor review procedures meet policy standards and are appropriate to the specific model.

Banks sometimes use third parties for validation when they purchase vendor models. The validation of the model theory, mathematics, assumptions, and code for purchased models can be complicated, as vendors sometimes are unwilling to share key model formulas and assumptions or program code with clients. In such cases, vendors typically supply clients with validation reports performed by independent parties. Such work can be relied on if management has adequate information to determine the scope is adequate and findings are appropriately conveyed to and acted on by the model vendor. Management may also increase its comfort with vendor-supplied models through a greater emphasis on regular outcome analysis. However, management cannot rely exclusively on a vendor's widespread industry acceptance as evidence of reliability.

Supervisory Evaluation of Model Use and Governance

Bank management is responsible for establishing an effective model governance program to recognize, understand, and limit the risks involved in the use of these important management tools. The examiner's role is to evaluate model use and governance practices relative to the institution's complexity and the overall importance of models to its business activities. Examiners incorporate their findings into their assignment of supervisory ratings to the bank.

For example, regulatory guidelines for rating the sensitivity to market risk component under the Uniform Financial Institutions Rating System include an assessment of management's ability to identify, measure, monitor, and control exposure to changes in interest rates or market conditions.[8] Any significant examiner concerns with the effectiveness of a model used to measure and monitor this risk, such as the failure to validate the model or a lack of understanding of model output, would have some negative effect on the rating. Conversely, if the model improves interest rate risk management, this would be positively reflected in the rating.

Other component ratings also can be influenced by model use, such as the evaluation of credit scoring models' effects on loan underwriting procedures and credit risk management in assigning an asset quality rating. The management component rating also may be influenced if governance procedures over critical models are weak.

The use of financial modeling in the banking industry will continue to expand. By necessity, supervisory attention to the adequacy of governance practices designed to assess and limit associated model risk also will increase.

Robert L. Burns, CFA, CPA
Senior Examiner

Potential bank governance practices and supervisory activities described in this article are consistent with existing regulatory guidance, but represent the thoughts of the author and should not be considered regulatory policy or formal examination guidance.

[8] Relative to the evaluation of a bank's sensitivity to market risk, the *FDIC Manual of Examination Policies* states, "While taking into consideration the institution's size and the nature and complexity of its activities, the assessment should focus on the risk management process, especially management's ability to measure, monitor, and control market risk" available at https://www.fdic.gov/regulations/safety/manual/section7-1.pdf.

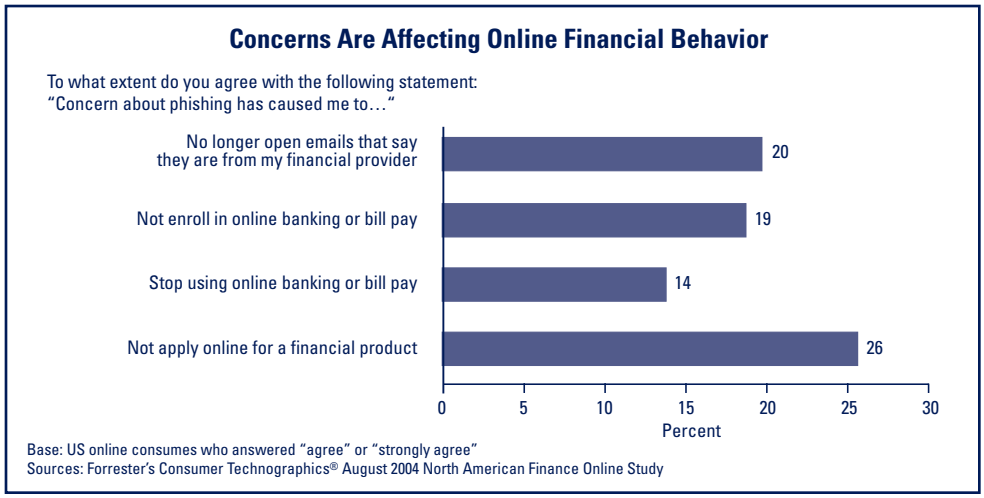
Online Delivery of Banking Services: Making Consumers Feel Secure

Much media attention recently has been focused on identity theft. Some of this publicity may suggest the Internet has evolved from a trusted tool for conducting research and legitimate business transactions to a medium whereby consumers' sensitive personal information can be stolen and used for criminal purposes. Social Security and credit card numbers, as well as bank account access data (such as passwords), are examples of some of the most sought-after information, providing perpetrators of identify theft access to bank balances and credit lines.

Many insured financial institutions rely heavily on the Internet to reach their customers, offering a wide variety of online banking services. In some cases, this practice has allowed banks and thrifts to consider scaling back brick-and-mortar facilities and staff required to conduct face-to-face banking transactions. However, security and privacy issues loom large in the minds of Internet users (see Chart 1). If financial institutions are to retain existing customers and attract new ones, they must create an online banking experience in which customers feel secure and have confidence their assets and personal information will not be compromised.

Highlighting another area of concern to customers of financial institutions, the results of a survey conducted by the ***Gartner Group*** in June 2005[1] show "the number of phishing attack e-mail recipients grew 28 percent this year....These and other breaches are exacting a steep toll on consumer confidence and will inhibit three-year e-commerce growth rates by 1 percent to 3 percent."[2] Issues concerning online users are highlighted in Chart 2, which emphasizes the level of concern about fraud and identity theft.

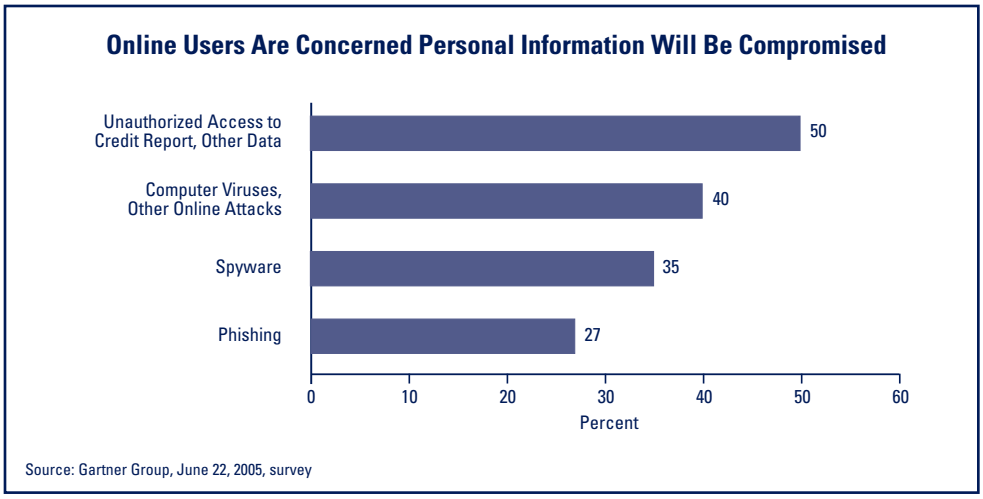
Chart 1



[1] Avivah Litan, "Increased Phishing and On-Line Attacks Cause Dip in Consumer Confidence," *Gartner* (June 22, 2005).

[2] The common phishing scenario is sending a fake e-mail (e-mail spoofing) purporting to come from a legitimate source and requesting information (such as a bank account number and password) or directing the victim to a fake Internet site where this information can be captured.

Chart 2



Concerns such as those identified in the Gartner Group survey and the high level of interest in preventing identity theft and safeguarding consumers' personal financial information prompted the FDIC to conduct its own study. The results of the study were released in mid-December 2004 in a publication entitled ***Putting an End to Account-Hijacking Identity Theft.***[3] The study has fostered debate among bankers, consumers, and regulators about how the risks posed by Internet-based financial services can be minimized. Following the publication of the study, the FDIC conducted several identity theft symposia featuring representatives from the banking industry, regulatory agencies, and consumer groups.[4] Participants considered the implications of conducting business on the Internet and initiatives for enhancing Internet security. Discussion focused on the areas of consumer privacy and protections, maintaining trust in the financial services industry, and the potential burden on smaller insured institutions that rely on external Internet service providers.

The overarching sentiment expressed during the symposia is that the problem of identity theft is not going away anytime soon. Although consumer protections are becoming more effective, hackers are becoming more sophisticated as well. In addition, while consumers want tightened security, they often are not willing to pay for it either through increased fees or any loss of convenience.

Many symposia participants recognized the banking industry must do a better job of self-regulating, for example, strengthening standards requiring companies to notify consumers whose data may have been lost or stolen. Participants acknowledged banks must do everything possible to prevent high-profile security breaches, such as those at ChoicePoint, LexisNexis, and Bank of America. Should more of these

[3] Federal Deposit Insurance Corporation, *Putting an End to Account-Hijacking Identity Theft* (December 14, 2004) available at https://www.fdic.gov/news/inactive-financial-institution-letters/2004/fil13204.html. A supplement to the study was released in June 2005 and is available at www.fdic.gov/news/news/financial/2005/fil5905.html. For purposes of this article, the results of the study and the supplement will be discussed as the results of the "study."

[4] The symposia were conducted in 2005 in Washington, D.C., (February 11), Atlanta (May 13), Los Angeles (June 17), and Chicago (September 22).

continued from pg. 13

incidents occur in the near term, the public may call for greater Federal government intervention, such as regulating where and how Social Security numbers are available on the Internet. Consumers also could be given the right to have their confidential information removed from computer systems of companies that have processed transactions for them or from systems maintained by data-brokering firms.

Another area of significant interest that emerged during the symposia relates to mitigating the level of risk inherent in conducting online transactions. Key questions posed during the symposia fall into four categories:

- **Risk reduction and risk mitigation** — What tools, policies, and procedures have proven most effective and can be considered best practices?
- **Risk transference** — Can insurance policies be designed to help protect consumers engaging in online financial transactions?
- **Risk acceptance** — Even though the goal of bankers and regulators is to minimize the level of risk inherent in online financial transactions, some level of risk always exists. How much risk are consumers willing to accept?
- **Risk avoidance** — How can the banking industry and regulators ensure consumers' confidential information is shared only with those who need it?

The following sections summarize the results of the FDIC study and key components of recently issued interagency guidance focusing on authentication[5] in an Internet environment.

What Level of Authentication Is Appropriate?

The FDIC study finds that traditional passwords consumers use to access their bank accounts via the Internet are too easily compromised and no longer represent an effective means to authenticate users. Once an Internet thief steals a password through phishing e-mails or other techniques, the consumer's accounts and personal information are at risk.

The study suggests a risk-based approach to identifying specific weaknesses in an insured institution's Internet banking system. For example, if online customers can view only non-sensitive information and are unable to transfer funds, the risk of harm to the customer is lower and, consequently, a less robust authentication method would be appropriate. On the other hand, if customers can transfer funds to other parties, this higher-risk transaction requires strong authentication procedures.

Authentication is based on the use of one or more of the following:

- Something you know, such as a password
- Something you have, such as an ATM card (a token)
- Something you are, such as a fingerprint (biometrics)

The vast majority of Internet-based financial services rely on single-factor authentication, usually a password, for customers to access their accounts. If an institution relies only on single-factor authentication, transactions are relatively easily compromised and lack adequate protection for sensitive consumer

[5] The process of identifying an individual traditionally based on a username and password. In security systems, authentication is distinct from authorization, the process of giving individuals access to system objects based on their identity. Authentication merely ensures the individual is who he or she claims to be, but says nothing about the individual's access rights.

information and funds. When a customer is tricked into disclosing a password, the thief could use the information to access the customer's accounts and potentially transfer funds.

A password combined with another form of authentication (i.e., two-factor authentication), such as an ATM card, provides much more reliable authentication. Multifactor authentication requires the user to supply at least one additional identification factor, such as a token-generated one-time password, USB token, smart card, or fingerprint.[6] Without the additional factor(s), a thief would not possess all credentials required to gain access to a customer's account. Therefore, multifactor authentication provides a more secure defense against identity theft.

The study describes one-time-password tokens, USB tokens, device authentication, geo-location, biometrics, and several other authentication technologies. The study also sheds light on how institutions may decide what technologies are right for them. Certain technologies present unique challenges. For example, the use of biometrics may not be appropriate for large, geographically dispersed customer bases. Biometrics (e.g., finger prints, iris structure, and facial features) are better suited to a captive audience, such as employees of a business housed in a single building. Insured financial institutions considering an authentication strategy should assess portability, ease of customer use, cost, effectiveness, ease of implementation, and the maturity of the technology.

In addition to discussing the shortcomings of traditional password authentication, the study concludes that financial institutions should

- Consider scanning software to identify and defend against phishing attacks;
- Strengthen education programs that advise customers about creating safe Internet experiences and recognizing attacks; and
- Continue to emphasize information sharing among the financial services industry, government, and technology service providers.

Regulators Work Together to Issue Guidance

Building on the results of the study and issues highlighted during the identity theft symposia, the Federal Financial Institutions Examination Council[7] (FFIEC) agencies issued guidance on October 12, 2005, entitled ***Authentication in an Internet Banking Environment.***[8] This guidance adopts the findings of the FDIC study relating to what constitutes effective customer authentication and recommends banks and thrifts offering Internet-based products and services use reliable and

[6] Tokens are small portable devices attached to a key ring carried by bank customers. One-time-password (OTP) tokens contain a small screen displaying several numbers. The token generates a random number every minute or so, which the customer enters into the online banking application. The financial institution receives the entered number and compares it with its records. A correctly entered number authenticates the customer and allows access. USB (universal serial bus) tokens, which can be plugged into the USB port of a bank customer's computer, contain unique identifying information that authenticates the customer.

[7] The Council is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the Federal examination of financial institutions by the Board of Governors of the Federal Reserve System (FRB), the FDIC, the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Office of Thrift Supervision (OTS) and to make recommendations to promote uniformity in the supervision of financial institutions.

[8] See FIL-103-2005: Financial Institution Letter "Authentication in an Internet Banking Environment" (October 12, 2005) available at https://www.fdic.gov/news/inactive-financial-institution-letters/2005/fil10305.html.

continued from pg. 15

effective methods to authenticate customers' identities. The authentication techniques explored should be appropriate to the risks associated with the products and services. As discussed previously, single-factor password based authentication is inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties. In these instances, insured institutions should use multifactor authentication, layered security,[9] or other appropriate controls.[10] Examiners may criticize institutions that have not properly mitigated risks identified in the assessment.

As insured financial institutions begin to assess their risks as outlined in the interagency authentication guidance, they should consider each type of transaction consumers can initiate online. The types of transactions may include the following:

- Access to the bank's website for new product offerings or CD rates
- Access to an individual deposit account
- Access to a deposit account and an automatic bill-paying option
- Ability to transfer money from one account to a related account
- Ability to transfer money to a third party

The above transactions are ranked by level of risk (beginning with the lowest level) they represent to the institution and the customer. The first transaction allows access only to general bank information; customer information or bank accounts cannot be accessed. This transaction is considered relatively low risk and would not require strong access controls.

However, the last transaction, which allows an online customer to wire or transfer money to another party, should require more than a password to initiate. In this case the bank should require the customer to supply authentication credentials such as a one-time password token. This layered approach to authentication matches low-risk transactions with less robust solutions and higher-risk transactions with stronger solutions. Risks falling in the middle would be addressed according to the potential for compromise of sensitive data or assets.

Insured financial institutions must comply with the interagency authentication guidance by December 31, 2006. To do so, they should begin performing risk assessments as soon as possible and, based on the results of these assessments, implement stronger authentication strategies by year-end 2006.

The FDIC and the other bank regulatory agencies are aware of the time and effort required to comply with the new authentication guidance. However, compliance with this guidance will help ensure that customers continue using an Internet delivery channel in which many banks and thrifts have invested a significant amount of capital.

Robert D. Lee
Senior Technology Specialist

[9] Layered security refers to the layers of risk, from low to high, as well as the layers of authentication implemented, from weak to strong. Layers of authentication processes are matched with corresponding layers of risk.

[10] See "Industry Initiatives" box at the end of this article for examples of industry initiatives targeted at deterring Internet theft and fraud, including the implementation of multifactor authentication procedures.

Industry Initiatives

During the past couple of years, a number of banks and technology service providers have implemented multifactor authentication products for Internet-based financial services. For example, E-bank, a large thrift, piloted a one-time password token program for its commercial customers during 2004 and has now made the tokens available to all its Internet banking customers. Bank of America recently implemented new software-based authentication technologies that provide its 13 million Internet banking customers with another authentication factor.[11] Multifactor authentication represents an effective strategy for protecting customers' funds and sensitive information, in addition to promoting confidence in Internet-based financial services.

Consumer education also is an effective deterrent to Internet theft and fraud. Many financial institutions disseminate brochures offering tips about avoiding scams and suggesting steps customers should take if they believe they have become victims. Consumers also are urged to use regularly updated antivirus software, firewalls, anti-spyware, and other tools to avoid having their personal information compromised.

[11] Daniel Wolfe, "Online Banks Are Taking to Authentication Tokens," *American Banker* (June 6, 2005).

Enforcement Actions Against Individuals: Case Studies

An article in the Summer 2005 issue of ***Supervisory Insights*** presented an overview of the enforcement action process as it relates to individuals and provided the statutory basis for administrative enforcement actions.[1] The article focused on fraud-related cases and noted that these cases generally fall into one of two categories: embezzlement or loan fraud. Although personal financial gain often was the motivating factor, a common aspect of a number of loan fraud cases was the desire to hide delinquencies or declining credit quality. The second in this series of articles builds on this information and presents two case studies that illustrate how embezzlement or loan fraud can occur, the effect it can have on an insured depository institution, and the importance of effective controls and oversight in helping prevent internal malfeasance.

Embezzlement Facilitated by Inadequate Internal Controls

A retail institution in a small city held less than $500 million in assets. The bank was consistently profitable. During a two-year period, a senior executive officer ("the officer") exerted significant influence over the loan function as well as the bank's operations. He had an authoritarian management style and was responsible for administration of more than half of the loan portfolio. The bank's board of directors had granted authority to the officer for a very high lending limit. Furthermore, the board usually reviewed and approved loans only after the fact, and delinquent-loan reports provided to the board were manually prepared by bank staff and subject to the officer's manipulation. The effects of the bank's inadequate internal controls and ineffective internal audit program were exacerbated by the officer's intimidation of employees and the bank's level of staffing, which did not keep pace with significant asset growth. Moreover, although senior management officials began to notice irregularities in the officer's activities, they failed to notify the board of directors, regulators, or law enforcement authorities in a timely manner, allowing the misconduct to continue.

The officer engaged in unsafe and unsound practices and breached his fiduciary duty to the bank. He committed a series of improper transactions involving customer loan or deposit accounts to fund his personal assets, improve his cash flow, and conceal his improper activities. The examples below describe a few of the instances of his misconduct.

- The officer extended a new loan to an existing bank customer to refinance a legitimate debt the customer owed to the bank. The settlement statement provided at closing was inconsistent with the amounts actually disbursed; that is, the statement reflected a loan payment that exceeded the actual amount paid. The officer used this difference and others to issue a cashier's check deposited in his account. The officer later used the proceeds to pay a personal debt and expenses, fund investments, and provide a loan payment for another borrower. All this was done without the first borrower's knowledge.

[1] Scott S. Patterson and Zachary S. Nienus, "Enforcement Actions Against Individuals in Fraud-Related Cases: An Overview," *Supervisory Insights,* Volume 2, No. 1 (Summer 2005).

- The officer established an unauthorized loan in the name of an existing bank customer and apparently forged the customer's signature. The officer used the loan proceeds to make a payment on a personal debt, pay personal expenses, make deposits in his personal accounts, and obtain cash.
- The officer made unauthorized advances on customers' legitimate, existing lines of credit. He advanced the unauthorized funds to make a deposit into one of his accounts and pay other personal expenses.
- The officer misappropriated funds from customer deposit accounts by transferring funds from a customer's account or depositing customer checks into his own account. The officer later reversed the misappropriations by transferring other, illegitimately obtained funds into the customers' accounts.

Through his misconduct, the officer acquired personal benefit of more than $1,000,000. However, the officer's misconduct combined with his efforts to conceal his activities resulted in losses of nearly $5,000,000 to the insured institution. Moreover, his departure left a significant void in management. Subsequently, the bank merged with another institution and no longer exists as an independent entity. The officer pled guilty to violations of Federal law, including embezzlement and misapplication of bank funds. The FDIC issued an Order of Prohibition against the officer to help ensure he does not participate in the affairs of another insured institution.

Loan Fraud Went Undetected Due to Lax Audit Function

Another consistently profitable retail institution in a small urban area held less than $500 million in assets. For nearly three years, a management official ("the officer") was alleged to have engaged in unsafe and unsound practices and to have breached his fiduciary duty to the bank by committing a series of improper transactions involving customer loan accounts. He initiated these transactions to cover delinquencies and credit problems.

The alleged misconduct involved hundreds of instances where loan accounts received illegitimate payments from improperly obtained funds. The bank's ineffective internal controls were a key contributing factor to these irregular activities. The officer was a trusted, long-time employee of the bank with reasonable lending authority; the seriousness of the situation was compounded by lax bookkeeping and scrutiny by one customer whose accounts he targeted. The officer initiated the advances and posted payments with only his signature and was authorized to correct "accounting errors." The bank's audit function failed to detect the alleged misappropriations in a timely manner.

Although the officer targeted one legitimate borrower for most of the wrongful advances, he used more than a dozen accounts as sources of funds. His scheme worked as follows. The officer made an advance from a current, performing loan (typically for less than $1,000) and applied the proceeds as payments to delinquent credits. The officer made improper advances of more than $150,000. The officer targeted one borrower who he knew had an active line of credit and did not scrutinize his transactions closely. When the targeted borrower questioned an advance, the officer blamed it on an "accounting error." He would then draw from another borrower's line of credit to cover the questioned advance. The delinquent borrowers who had

continued from pg. 19

payments applied to their loans apparently had no knowledge of the officer's activities.

Although this officer did not personally benefit from his wrongdoing, other than possibly maintaining his position at the bank, the insured institution incurred credit losses and costs for investigating the misconduct. The problem credits paid off through the misappropriated funds required extensive collection efforts because the bank had previously released any collateral when the loan was fraudulently extinguished. In addition, by making improper payments on the delinquent loans, the officer prevented the bank from recognizing the borrowers' problem status and taking remedial action. These illegitimate payments also resulted in inaccurate financial statements and erroneous regulatory reports. The FDIC issued an Order of Prohibition against the officer, preventing him from moving to another institution.

The Bottom Line

These case studies illustrate what the FDIC may face as it carries out its supervisory obligations. Although the two officers' motivations differed, the effect was the same — both financial institutions suffered monetary losses and investigation costs. Long-time bank employees in a position of trust exploited internal control weaknesses to conduct improper activities. This situation was exacerbated when one employee was able to intimidate other employees into cooperating. Proper controls and oversight must be in place to help prevent internal malfeasance, and timely response by management is needed to limit the impact. An effective audit program (components of which appear in the shaded text box on the next page) can help identify and deter wrongdoing.

Scott S. Patterson
Review Examiner

Internal Audit

The internal audit function is a critical element in assessing the effectiveness of an institution's internal control system. The internal audit consists of procedures to prevent or identify significant inaccurate, incomplete, or unauthorized transactions; deficiencies in safeguarding assets; unreliable financial reporting; and deviations from laws, regulations, and institution policies. When properly designed and implemented, internal audits provide directors and senior management with timely information about weaknesses in the internal control system, facilitating prompt remedial action. Each institution should have an internal audit function appropriate to its size and the nature and scope of its activities. The FDIC has adopted minimum standards for an internal audit program.[2]

In addition, ***The Interagency Policy Statement on the Internal Audit Function and Its Outsourcing***[3] discusses, among other things, key characteristics of the internal audit function. Although the board of directors and senior management cannot delegate responsibility for an effective internal control system and audit function, they may delegate the design, implementation, and monitoring of specific internal controls to lower-level management and the testing and assessment of internal controls to others. An institution's internal audit function should address the following.

Structure — The internal audit function should be positioned within an institution's organizational structure to allow staff to perform their duties impartially. The audit committee[4] should oversee the internal audit function, evaluate performance, and assign responsibility for this function to a member of management (the internal audit manager). The internal audit manager should understand the internal audit function, but have no responsibility for operating the internal control system. For example, the internal audit manager should not approve or implement an institution's operating policies. Ideally, the internal audit manager should report directly to the audit committee about audit issues and administrative matters (e.g., compensation or budgeting).

Management, Staffing, and Audit Quality — The internal audit function should be supervised and staffed by employees with sufficient expertise and resources to identify the risks in an institution's operations and to assess the adequacy and effectiveness of internal controls. The internal audit manager should oversee audit staff and establish appropriate internal audit policies and procedures. The internal audit manager is responsible for the following:

- A control risk assessment documenting the internal auditor's understanding of significant business activities and associated risks. These assessments typically analyze the risks inherent in a given business line, the mitigating control processes, and the resulting residual risk exposure.
- An internal audit plan responsive to results of the control risk assessment. This plan typically specifies key internal control summaries within each business activity, timing and frequency of internal audit work, and the resource budget.
- An internal audit program that describes audit objectives and specifies procedures performed during each internal audit review.
- An audit report presenting the purpose, scope, and results of the audit. Work papers should be maintained to document the work performed and support audit findings.

Scope — The frequency and extent of internal audit review and testing should be consistent with the nature, complexity, and risk of an institution's on- and off-balance-sheet activities. The audit committee and management should conduct a cost-benefit analysis to determine the appropriate extent of the audit function. A small institution without an internal auditor can maintain an objective internal audit function by implementing a comprehensive set of independent reviews of significant internal controls by person(s) not responsible for managing or operating those controls. At least annually, the audit committee should review and approve the internal audit's control risk assessment and the scope of the audit plan (including any reliance on an outsourcing vendor). The audit committee also should periodically review the internal audit staff's adherence to the audit plan and consider requests for expansion of audit work when significant issues arise or when substantive changes occur in an institution's environment, structure, activities, risk exposures, or systems.

Communication — Internal auditors should immediately report internal control deficiencies to the appropriate level of management, and should report significant matters directly to the board of directors or the audit committee and senior management. The audit committee should give the internal audit manager the opportunity to discuss his or her findings without management being present, and the audit committee should establish procedures allowing employees to submit concerns about questionable accounting, internal accounting control, or auditing matters confidentially and anonymously.

Contingency Planning — Insured institutions should develop and implement a contingency plan to address any significant discontinuity in audit coverage, particularly for high-risk areas.

[2] 12 CFR Part 364, Appendix A, FDIC Rules and Regulations, Interagency Guidelines Establishing Standards for Safety and Soundness.

[3] FIL-21-2003: Financial Institution Letter, "Interagency Policy Statement on the Internal Audit Function and its Outsourcing" (March 17, 2003).

[4] Depository institutions subject to Section 36 of the Federal Deposit Insurance Act and Part 363 of the FDIC's regulations must maintain independent audit committees composed of directors who are not members of management. The FDIC encourages the board of directors of each depository institution not required to do so by Section 36 to establish an audit committee consisting entirely of outside directors.

From the Examiner's Desk… The FDIC's Relationship Manager Program: A Win/Win Situation

This regular feature focuses on developments that affect the bank examination function. We welcome ideas for future columns, and readers can e-mail suggestions to ***SupervisoryJournal@fdic.gov.***

Consider this scenario: Every FDIC-supervised institution has a local point of contact, a Relationship Manager who is familiar with the institution's financial condition, operations, management team, and local economic environment. Bank management meets with its Relationship Manager, who is also available by phone or e-mail to get answers to questions about regulatory issues or examination scheduling. This scenario is happening right now. The agency implemented the Relationship Manager Program on October 1, 2005, to further strengthen relationships between the FDIC and bank management and continue to improve the effectiveness of the supervisory process.[1]

FDIC Pilot: Building a Successful Program

The FDIC's Division of Supervision and Consumer Protection piloted the Relationship Manager Program with 390 banks in eight states across the country beginning in April 2004. Coordination with State banking authorities is always critical; consequently, the FDIC sought and received cooperation from each State banking department involved in the pilot (see inset box on next page). The pilot addressed three key principles of the Program: (1) a Relationship Manager is the local point of contact for each FDIC-supervised institution; (2) supervisors have the flexibility to conduct examination activities over the examination cycle;[2] and (3) a Risk Management Consolidated Report of Examination will cover Risk Management, applicable specialty areas, and, if the findings are significant, Compliance and the Community Reinvestment Act (CRA). As expected with any pilot program, some adjustments were necessary (as explained below). Feedback was positive, and the pilot was continued until the Program was implemented nationwide in October 2005.

Relationship Managers: Key to the Success of the Program

Commissioned examiners[3] are assigned as the Relationship Manager for four to six banks, and their role is paramount in the Program. (See inset box "Perspectives from an FDIC Examiner" for the views of one examiner who is now a Relationship Manager.) The Relationship Manager has three primary responsibilities. First, the Relationship Manager is the institution's local point of contact —

[1] See FIL-98-2005: Financial Institution Letter "Relationship Manager Program Enhancements to the Supervision Program" (October 6, 2005). This FIL states that (1) all FDIC-supervised institutions will have an assigned local point of contact; (2) the Relationship Manager Program will enable examiners to conduct interim examination activities; (3) financial institutions will receive a Report of Examination that incorporates all Risk Management and specialty examination findings during an examination cycle; (4) separate Compliance/Community Reinvestment Act frequency requirements and reports will continue to be issued, but examination activities will be closely coordinated with other supervisory activities; and (5) separate examination cycles for specialty examinations are now integrated into the Risk Management examination cycle.

[2] 12 USC 1820 (d) requires FDIC-insured institutions to be examined every 12 or 18 months, depending on size and financial condition. This 12- or 18-month period is referred to as the institution's "examination cycle."

[3] FDIC examiners must complete a training program consisting of on-the-job training, classroom sessions, and a technical evaluation. The commissioning process generally takes three years, and Compliance and Risk Management examiners can begin serving as Relationship Managers approximately one year after being commissioned.

Coordination with State Banking Departments: A Key Aspect of the Relationship Manager Program

The FDIC is the primary Federal regulator for State-chartered nonmember banks, and supervision of these banks is a partnership effort between the FDIC and the respective State banking departments. For the most part, examinations are conducted on a rotating basis by the FDIC and the State. Agreements between the FDIC and each State banking department specifying examination responsibilities are in place, and financial institutions will continue to be supervised according to these agreements.

Communication and coordination with State authorities was critical in the development of the Relationship Manager Program. To facilitate secure communication with the State banking departments, the FDIC worked with State banking supervisors to develop technological solutions that foster the sharing of confidential information. The importance of this secure network to an initiative that relies on coordination between the FDIC and the State banking authorities cannot be overstated. To facilitate communication with State authorities, copies of supervisory plans will be provided, and State examiners will continue to have access to FDIC work papers. Relationship Managers will contact State officials according to the protocol established by the FDIC Regional Office and that State.

a direct resource for bank management's questions about regulatory issues or new bank products. During the pilot, bankers reported that their Relationship Manager generally understood their bank's operations and could provide valuable supervisory insights.

Second, the Relationship Manager develops a supervisory plan at the beginning of the examination cycle which includes a risk assessment of the institution and a supervisory agenda and timeline. This plan incorporates Risk Management, Compliance, and CRA, as well as specialty areas such as Information Technology, Trust, Registered Transfer Agent, Municipal Securities Dealer, and Government Securities Dealer. The plan establishes the overall supervisory approach for the institution and documents examination and off-site monitoring activities scheduled during that cycle. Most banks are examined on a rotating basis by the FDIC and the chartering State authority. During the State authority's examination cycle, the Relationship Manager will prepare an abbreviated supervisory plan listing the State's proposed examination date and any off-site monitoring events scheduled during the period. In cases where the State authority does not examine for Bank Secrecy Act (BSA) compliance, the supervisory plan will address plans for the FDIC to conduct a separate BSA/Anti-Money Laundering examination.

Finally, Relationship Managers participate in examinations of their assigned institutions. Generally, the Relationship Manager will be the examiner-in-charge for his examination discipline (such as Risk Management or Compliance/CRA) or will serve in a prominent role and work closely with the examination staff. However, if the Relationship Manager is not available, another commissioned examiner could serve as the examiner-in-charge, with the Relationship Manager participating in the examination to the extent possible. During the pilot, examiners and bankers recognized the benefit of the Relationship Manager serving as the examiner-in-charge or, at the very least, in an important role during the examination. Mark Yates, Field Supervisor for the FDIC's Columbus, Ohio, Field Office, stated that having the Relationship Manager participate in the examination "provided for the Relationship Manager's continued awareness of the institution and resulted in a more effective and better focused examination." However, having a different examiner serve as the examiner-in-charge may foster objectivity if the Relationship Manager has dealt with the bank for some time. Examiner independence is

continued from pg. 23

crucial, and field supervisors will rotate examiner-in-charge assignments periodically to ensure fair and objective treatment for all institutions.

Flexibility and Communication Improve the Supervisory Process

The Relationship Manager Program does not change examination procedures. Rather, it promotes flexibility in, and emphasizes coordination of, examination activities and strengthens lines of communication between bankers and the FDIC. During the pilot, examination staff experimented with conducting examination activities throughout the examination cycle instead of relying on a single point in time examination at the end of the cycle.

Under this approach, the examiner does not have to wait until the next examination begins to assess management's response to significant examination concerns and issues, resulting in more timely communication about areas of regulatory concern. Performing certain examination activities throughout the cycle also helps the FDIC use personnel and respond to bankers' needs efficiently. For example, field supervisors periodically receive banker requests to reschedule an examination owing to a computer conversion or other planned events that significantly impact operations. This flexible examination approach facilitates these requests by allowing interim examination activities to be conducted rather than having to reschedule an entire examination.

Conducting interim examination activities was found to be especially beneficial in large, complex institutions. For example, a partial loan review was conducted at an institution that purchases large pools of problem loans. The examiners conducted their review 60 to 90 days after the pools were purchased, allowing for the seasoning of the loans and therefore a more effective review of the quality of the portfolio. Although this flexibility remains in the Program, this approach will not be the norm. During the pilot, we determined that for the vast majority of institutions, particularly small, less complex institutions, a point in time examination remains the most efficient approach.

The Relationship Manager's knowledge of a specific bank's operations also should improve the overall effectiveness and efficiency of the FDIC's supervision program. For example, if a bank reports significant quarterly growth in deposits, the Relationship Manager may have information about a new product that the bank was developing, and, as a result, only limited supervisory follow-up may be necessary. This follow-up may present an opportunity for the Relationship Manager to call on bank management to review the product's success or discuss potential regulatory considerations that may be prompted by the deposit growth.

Risk Management Consolidated Report of Examination: A Comprehensive, Consistent Message

The use of one consolidated Report of Examination for Risk Management, specialty examination areas, and Compliance/CRA was tested during the pilot. Based on the success of the pilot, separate reports for specialty areas — such as Information Technology, Trust, Government Securities Dealers, and Municipal Securities Dealers — generally no longer will be completed; examination findings for specialty areas now will be detailed in the Risk Management Consolidated Report of Examination (Consolidated Report). However, incorporating Risk Management and Compliance/CRA

Perspectives from an FDIC Examiner

As a commissioned Risk Management examiner, I have been involved in the Relationship Manager Program since April 2004. I was initially assigned a portfolio of six banks. One of my first duties as a Relationship Manager was to contact each bank, inform management that I was now the local point of contact, and describe the Program and its benefits. Initial reaction from bankers was favorable, and the Program continues to be well received. When asked if "having a Relationship Manager as the designated local point of contact improves the relationship between the institution and the FDIC," 69 percent of responding bankers strongly agreed and 28 percent somewhat agreed.

Bankers particularly like the opportunity to address their concerns to someone familiar with their unique situation, and, in fact, many bankers frequently call and e-mail me. Some questions are outside my area of expertise; however, I identify a subject matter expert and ensure the bank's questions are answered. When bankers feel comfortable asking questions, the potential for problems to occur down the road is minimized.

The development of supervisory plans requires strong communication with examiners working in other disciplines. As a result, information sharing between myself and Compliance examiners has increased significantly. For example, a Compliance examiner recently finished an examination at one of the banks in my portfolio. He informed me that the Compliance examination revealed significant violations of Part 339 — Flood Insurance, which resulted in proposed civil money penalties. The information helped me assess the institution's overall risk profile before I conducted the Risk Management examination.

The FDIC and the West Virginia Division of Banking (WVDOB) have always worked well together. We share work papers, discuss institution-specific concerns, and coordinate examination activities; the Relationship Manager Program strengthened this partnership. The WVDOB previously developed a similar program designating a State examiner as a "CPC" (central point of contact) for each State-supervised insured financial institution. Regular contact with the State examiner helps me gather information about the environment in which a particular bank operates as well as its overall risk profile.

The Relationship Manager Program has enhanced my understanding of the insured institutions in my portfolio and has strengthened my communication with bank management and State banking authorities. Bankers express their appreciation for the FDIC's willingness to listen and respond to their concerns, and the Program has fostered in me a sense of "ownership" of banks in my portfolio. This is indeed a "win/win" situation for the FDIC, insured institutions, and State regulators.

Dan Langdon
Examiner, Scott Depot, West Virginia, Field Office

findings into one consolidated Report of Examination proved more difficult. Compliance/CRA and Risk Management examinations may need to be conducted at different times during the cycle, and consolidating Compliance/CRA and Risk Management into one Report of Examination would delay the transmission of important examination findings to bank management. Therefore, separate Compliance/CRA reports will still be prepared but material findings contained in the Compliance/CRA Report of Examination will be summarized in the Consolidated Report. Consolidating examination findings for Risk Management and specialty areas, including material Compliance/CRA findings, will provide a bank's board a comprehensive overview of the risks and regulatory issues facing the institution. The Consolidated Report also will include the assigned ratings for Risk Management, Compliance, CRA, and any applicable specialty areas.

Coordination of all aspects of a bank's supervision and the use of a supervisory plan and Consolidated Report should improve coordination and consistency of message among examination disciplines. For example, Risk Management examiners will be more aware of an institution's Compliance risks and how they may

continued from pg. 25

affect its overall risk profile. In turn, Compliance examiners become more familiar with the institution's operations and related risks in specialty areas, such as Information Technology and Trust.

An Evolving Relationship between Banks and Supervisors

The FDIC's Relationship Manager Program is a natural next step in the evolution of the relationship between banks and regulatory agencies. Although their perspectives may at times differ, bankers and regulators generally have a common objective: safe, profitable institutions that provide fair and reliable service to consumers. Bank management now will benefit from having a local point of contact at the FDIC familiar with the institution's operations and overall risk profile. The Consolidated Report will provide the board with a comprehensive view of the bank's condition and outstanding supervisory issues. The flexibility fostered by the Program will improve the quality, continuity, and timeliness of the supervisory process and promote the efficient use of FDIC resources. Finally, everyone will benefit from enhanced communication between bankers and the FDIC.

Louis J. Bervid III
Senior Examination Specialist

The author acknowledges the assistance provided by the following individuals in the preparation of this article:

Members of the FDIC's Relationship Manager Development Group

Julie D. Howland
Special Assistant to the Deputy Director of Special Projects, Division of Supervision and Consumer Protection

Daniel J. Langdon
Examiner, Scott Depot, West Virginia, Field Office

Capital and Accounting News . . . Basel II and the Potential Effect on Insured Institutions in the United States: Results of the Fourth Quantitative Impact Study (QIS-4)

This regular feature focuses on critical bank capital and accounting issues. Comments on this column and suggestions for future columns may be e-mailed to ***SupervisoryJournal@fdic.gov.***

The Basel II Capital Accord represents a major shift in international capital policy. As Europe moves rapidly ahead with its legislative process to adopt Basel II, attention has focused on U.S. implementation. Some commentators have criticized the U.S. Basel II implementation process for being both slower in pace and more conservative in its approach to required capital than the approach taken across the Atlantic. This article reviews some of the highlights of the U.S. banking agencies' recent capital impact study to provide some context to the agencies' recently announced implementation plans.

On September 30, 2005, the U.S. agencies announced a revised timeline for moving ahead with the implementation of Basel II in the United States.[1] The revised plan includes more time to implement the framework and floors on banks' risk-based capital requirements during a three-year transitional period. The revised plan was driven in substantial part by the results of the agencies' recent *Quantitative Impact Study* (QIS-4). Specifically, at present the Basel II framework appears likely to recommend capital levels that may not be sufficient to address the risks banks face. It also appears likely there will be substantial challenges in implementing the framework consistently across banks. The agencies have indicated that to address such issues, future changes to the framework are likely.

Evolution of Capital Standards

The 1988 Basel I Accord was the first attempt at capital regulation that produced risk-based capital requirements. It represented a significant change from earlier standards. Throughout the 1990s, a shift has occurred in banking regulation that further enhances the risk sensitivity of capital requirements. In 1996, as market risk management techniques evolved, a models-based, risk-sensitive approach was established for banks and bank holding companies conducting significant trading activity. The Market Risk Rule was based on value-at-risk measures used by the most sophisticated market practitioners; it created a separate market risk capital charge equal to the banks' internal calculations. Similarly, credit and operational risk advancements have been incorporated into the proposed Basel II framework to better assess capital charges related to underlying risk and align regulatory capital with internal capital allocation methodologies.

During the development of the proposed Basel II framework, the Basel Committee on Banking Supervision (Basel Committee) published three consultative papers for the purpose of incorporating enhancements to the framework. Domestically, the U.S. banking regulatory agencies released an Advance Notice of Proposed Rulemaking (ANPR) in August 2003.[2] Shortly thereafter, the participating countries agreed to the Madrid Proposal, which introduced a fundamental shift in capital policy toward an unexpected-loss (UL)-based framework (a concept of

[1] Joint Press Release, Board of Governors of the Federal Reserve, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency, Office of Thrift Supervision, Banking Agencies Announce Revised Plan for Implementation of Basel II Framework (September 30, 2005) available at www.fdic.gov/news/news/Press/2005/pr9805.html.

[2] This document is available at www.fdic.gov/regulations/laws/publiccomments/ANPR.html.

continued from pg. 27

capital to be held for unexpected losses only, with expected losses covered by reserves).[3] In June 2004, the Basel Committee published the ***International Convergence of Capital Measurement and Capital Standards: A Revised Framework,*** also known as the Mid-Year Text, which will serve as the basis for national implementation of the Basel II framework. Currently, the U.S. banking regulatory agencies are drafting the Notice of Proposed Rulemaking (NPR), as well as guidance for the various portfolios, to apply the Mid-Year Text domestically.

Principles of Basel II

The new capital framework establishes a "three-pillar" approach to bank capital regulation:

- Pillar 1 sets the standards for computing regulatory capital requirements, consisting of credit, market, and operational risk.[4]
- Pillar 2 is a supervisory review process that examines factors not considered under Pillar 1, such as board oversight, internal controls, and assessment of risk to ensure capital adequacy.
- Pillar 3 encourages market discipline through a public disclosure process.

In addition, Basel II differs from the current framework in various ways. Operational risk was implicit in the capital requirement under Basel I; however, separate operational risk and credit risk capital charges exist under Basel II. Changes also have been made in the measurement of credit risk. Instead of a flat, 100 percent risk weight for corporate exposures regardless of actual risk, Basel II enhances risk sensitivity by focusing on differences among individual credits recognized through banks' internal ratings.[5] A similar approach is applied to retail portfolios, in which capital is assigned to segments based on various loan characteristics.

Various risks are not captured under the Pillar 1 requirements. The proposed framework quantifies only credit, operational, and market risk, strengthening the need to retain the leverage ratio for the Pillar 1 requirements, as the computed capital requirements for these risks will be lower than if all risks were captured. Interest rate risk, liquidity risk, and concentration risk, among others, are not included in minimum regulatory capital. These risk categories must be considered in the "assessment of risk" under Pillar 2. The quantitative impact studies have focused solely on Pillar 1 requirements.

Quantitative Impact Studies

Significant differences exist between Basel I and Basel II. Therefore, regulators must determine and evaluate the potential effects before new capital policy is enacted. As a result, quantitative studies have been designed to measure the change in capital likely to occur once the proposed framework is implemented. Various studies have been completed during the past five years, both domestically and internationally. The third *Quantitative Impact Study* (QIS-3), undertaken internationally in 2002, showed a decline of roughly

[3] Basel Committee on Banking Supervision, *Madrid Proposal,* October 10, 2003, available at www.bis.org.

[4] Various approaches for credit and operational risk are allowed under the framework, but only the advanced approaches will be implemented in the United States at the largest, most complex institutions.

[5] *Economic Capital and the Assessment of Capital Adequacy, Supervisory Insights,* Winter 2004, (description of internal ratings and the Basel II Pillar 1 computation), available at https://www.fdic.gov/regulations/examinations/supervisory/insights/siwin04/siwinter04-article1.pdf.

6 percent in minimum required capital (MRC) among U.S. participants.

The most recent quantitative impact study, QIS-4, began in fourth quarter 2004 and consisted of instructions, a workbook for data collection, and a quality questionnaire to assist in understanding the methodologies behind the results. Twenty-six institutions, including banks and consolidated bank holding companies, submitted materials during first quarter 2005. This group of institutions represented more than 57 percent of banking assets and roughly 44 percent of insured deposits. The aggregate QIS-4 results for these institutions are shown in Table 1 and described below.

QIS-4 Shows Significant Decline in Capital Levels

In aggregate, the sample reported an average decline of 15.5 percent in minimum capital requirements compared with the current framework

Table 1

Preliminary Change in Minimum Capital Requirements: Basel I to Basel II

Portfolio	Average Percent Change in Portfolio MRC	Median Percent Change in Portfolio MRC
Wholesale Credit	**(24.6%)**	**(24.5%)**
Corporate, Bank, Sovereign	(21.9%)	(29.7%)
Small Business	(26.6%)	(27.1%)
High Volatility Commercial Real Estate	(33.4%)	(23.2%)
Income Producing Real Estate	(41.4%)	(52.5%)
Retail Credit	**(25.6%)**	**(49.8%)**
Home Equity (HELOC)	(74.3%)	(78.6%)
Residential Mortgage	(61.4%)	(72.7%)
Credit Card (QRE)	66.0%	62.8%
Other Consumer	(6.5%)	(35.2%)
Retail Business Exposures	(5.8%)	(29.2%)
Equity	6.6%	(24.4%)
Other Assets	(11.7%)	(3.2%)
Securitization	(17.9%)	(39.7%)
Operational Risk		
Trading Book	0.0%	0.0%
Portfolio Total	**(12.5%)**	**(23.8%)**
Change in Effective MRC	**(15.5%)**	**(26.3%)**

This is the change in the amount of Tier 1 capital and Tier 2 elements other than reserves needed to meet the minimum capital requirement.

MRC = minimum required capital

Operational risk, a new measure reported under Basel II, represented roughly 10.5 percent of the Basel II capital charge. Because the Market Risk Rule amended domestic capital rules in 1996, capital requirements for the trading book remained unchanged at the time QIS-4 was conducted. Since that period, a number of trading book modifications have been made to the Basel II framework following work by the Basel/International Organization of Securities Commissions (IOSCO) group. However, the effects of these changes are unknown pending further domestic analysis and the results of the next impact study.

continued from pg. 29

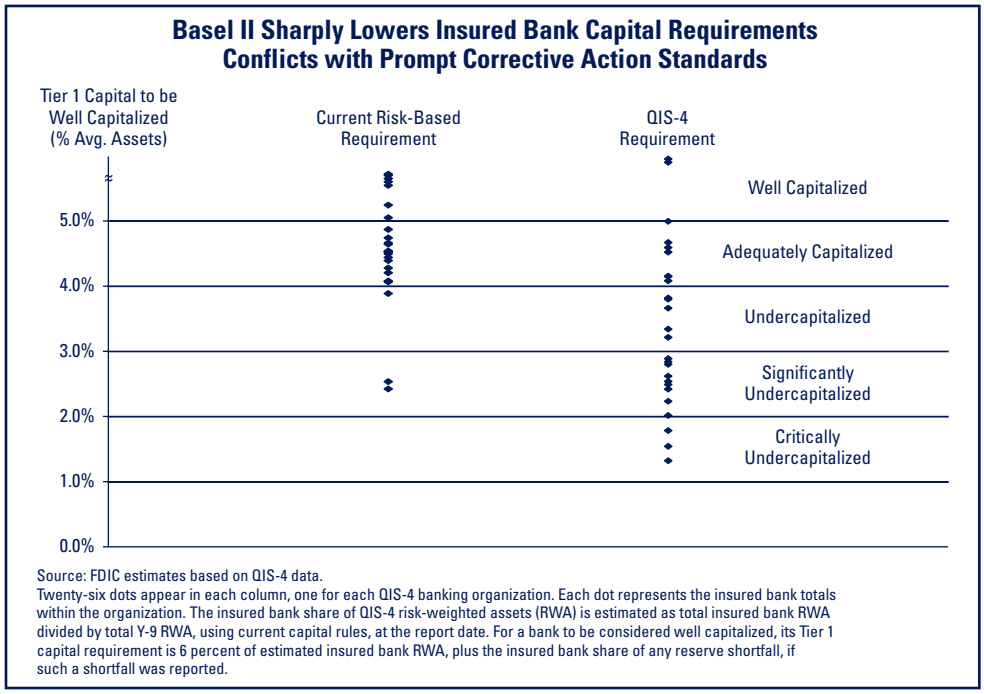
(see Figure 1). The *median* decline in regulatory capital was even more dramatic at 26.3 percent, as a few of the larger participants weighted the average higher. The greatest contributors to this decline were the corporate, bank and sovereign, residential mortgage, and home equity portfolios. Only credit card and equity portfolios showed increases in minimum capital requirements under the new framework.

Recent FDIC analysis of QIS-4 indicates the leverage ratio would become the binding constraint for most QIS-4 participants as their Basel II minimum capital requirements generally fell substantially below current Prompt Corrective Action thresholds. The FDIC views the QIS-4 levels of capital reported by many participating institutions as inadequate, as noted in recent congressional testimony.[6]

QIS-4 Also Shows Significant Dispersion

The overall QIS-4 results reveal not only a decline in aggregate capital requirements, but also a wide dispersion of capital requirements among the participants and the various portfolios. Although some variation in results can be expected as a result of differences in risk profiles across institutions, the extent of variance shown in QIS-4 is cause for concern. Changes in effective MRC ranged from a 47 percent decline to a 55 percent increase across institutions. Within portfolios, wholesale requirements ranged from a decline of 80 percent to an increase of 56 percent. All institutions in the study would experience a drop in capital held for residential mortgages under Basel II, with declines ranging from 18 percent to 99 percent (see Appendix).

Figure 1



Source: FDIC estimates based on QIS-4 data.
Twenty-six dots appear in each column, one for each QIS-4 banking organization. Each dot represents the insured bank totals within the organization. The insured bank share of QIS-4 risk-weighted assets (RWA) is estimated as total insured bank RWA divided by total Y-9 RWA, using current capital rules, at the report date. For a bank to be considered well capitalized, its Tier 1 capital requirement is 6 percent of estimated insured bank RWA, plus the insured bank share of any reserve shortfall, if such a shortfall was reported.

[6] Donald Powell, Chairman, Federal Deposit Insurance Corporation, Testimony Before the Senate Banking Committee (testimony focused on U.S. implementation of Basel II Framework), November 10, 2005, available at www.fdic.gov/news/news/speeches/chairman/spnov1005.html.

Within benchmarking studies of corporate credits and mortgage loans on QIS-4 data, the agencies found that loans with the same or similar characteristics were assigned very different risk parameters, and consequently were receiving materially different capital requirements under QIS-4. Publication of guidance, the rulemaking process, and further development of bank systems to conform to regulatory standards will address some of the dispersion; however, variability is inherent in the proposed capital framework and may need to be addressed.

Extended Analysis

Due to concern with the magnitude of the decline and the dispersion of the initial results, the U.S. banking agencies issued a press release on April 29, 2005, suggesting further analysis be performed before publication of the NPR.[7] To clarify these issues, additional work has focused on determining whether the results reflect differences in risk, reveal limitations of QIS-4, identify variations in the stages of bank implementation efforts (particularly related to data availability), or suggest the need for adjustments to the Basel II framework.

Additional analysis focused on benchmarking select portfolios, a qualitative questionnaire review, and sensitivity analysis for the top six or seven mandatory institutions participating in the study, as these institutions are believed to be further along in the implementation process. The results of the analysis suggest that the level of decline is explained in part by the economic cycle resulting from the inherent risk sensitivity of the new Basel II accord and the strong economic conditions in the United States at the time of the study. With regard to the dispersion, the assessment of risk parameters resulting from differences in banks' data and methodologies, as well as portfolio mix, contributed to the variation. It is possible that limitations in QIS-4 instructions, which were based on draft guidance and the Mid-Year Text, contributed to the results as well.

Next Steps

The additional QIS-4 analysis has been completed and will be communicated to the industry and the Basel Committee, although further analysis may be needed to address issues raised during QIS-4. QIS-5 will be completed internationally during fourth quarter 2005,[8] and the effects of the proposed framework on capital levels across all countries will be analyzed in 2006 to determine if changes to the framework are warranted. In addition, the Basel Committee has tasked a Dynamic Operations Project team, consisting of a small group of international bank regulators, to examine the effects of cyclicality on Basel II capital requirements. Results are due back to the Basel Committee in 2006.

As the U.S. rulemaking process was delayed until the QIS-4 analysis was completed, the U.S. agencies are currently discussing options for the timing of the NPR and domestic implementation. The regulators are committed to working through issues to continue with Basel II implementation in the United States.

Andrea Plante
Senior Quantitative Risk Analyst

[7] Joint Press Release, Board of Governors of the Federal Reserve, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency, Office of Thrift Supervision, Banking Agencies To Perform Additional Analysis Before Issuing Notice of Proposed Rulemaking Related To Basel (April 29, 2005), available at www.fdic.gov/news/news/press/2005/pr3705.html.

[8] The United States will not participate in QIS-5. Most countries other than the United States, Germany and Japan did not participate in QIS-4, but rather waited until 2005 to complete an impact study. The U.S. QIS-4 results will be rolled into the international analysis.

continued from pg. 31

Appendix

Figure A-1

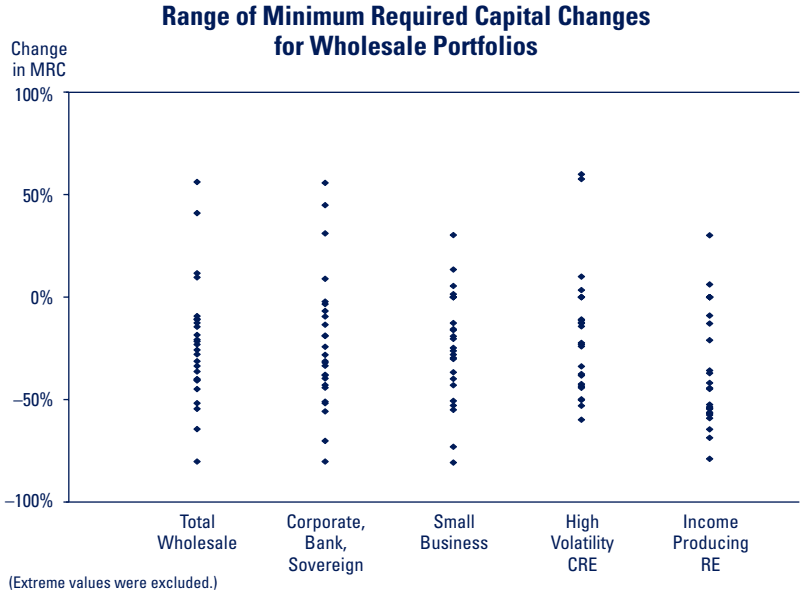
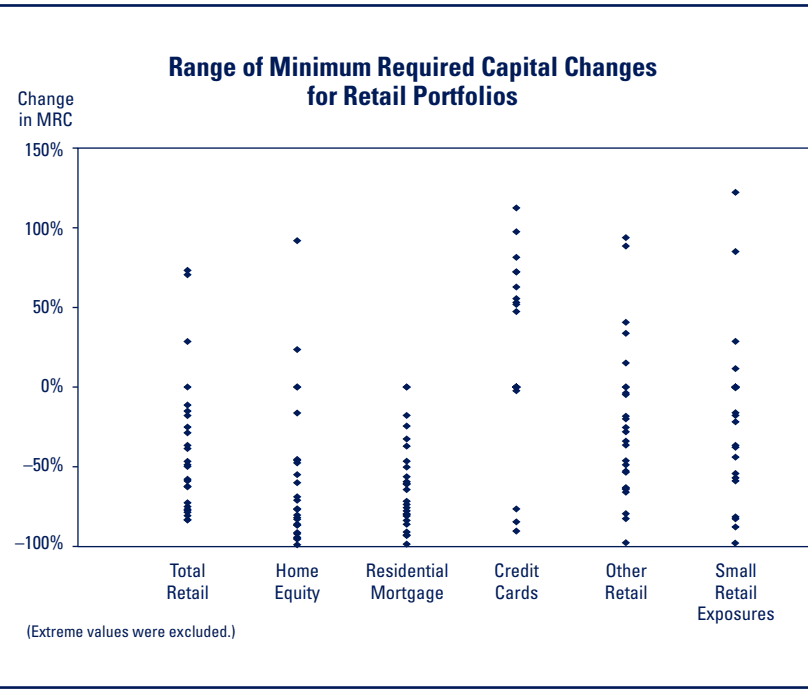


Figure A-2



Overview of Selected Regulations and Supervisory Guidance

This section provides an overview of recently released regulations and supervisory guidance, arranged in reverse chronological order. Press Release (PR) or Financial Institution Letter (FIL) designations are included so the reader may obtain more information.

Subject	Summary
Assistance to Financial Institutions and Customers Affected by Hurricanes	Various initiatives have been implemented to reduce regulatory burden on financial institutions in areas recently affected by hurricanes. These include providing flexibility in the administration of regulatory requirements for brokered deposit waivers, main office and branch relocations and closings, and appraisals. Other ongoing efforts to assist financial institutions and their customers include establishing regulatory agency hotlines, issuing guidance to assist with the recovery process, and disseminating critical information on the regulators' websites. The Federal Financial Institutions Examination Council (FFIEC) announced the formation of an interagency Supervisory Policy Working Group on September 19, 2005, to enhance the agencies' coordination and communication on, and supervisory responses to, issues facing the banking industry in the aftermath of the recent hurricanes. The FFIEC's website (www.ffiec.gov/katrina) provides links to all member agencies' websites where additional information is available.
Comments Requested on Suggested Domestic Risk-Based Capital Modifications (PR-105-2005 and *Federal Register,* Vol. 70, No. 202, page 61068, October 20, 2005)	The four Federal banking agencies (the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation [FDIC], the Office of the Comptroller of the Currency [OCC], and the Office of Thrift Supervision [OTS]) published an interagency Advance Notice of Proposed Rulemaking regarding potential revisions to the existing risk-based capital framework. These changes would apply to banks, bank holding companies, and savings associations. Comments must be received by January 18, 2006.
Authentication in an Internet Banking Environment (FIL-103-2005, October 12, 2005)	The Federal financial institution regulatory agencies (the Board of Governors of the Federal Reserve System, the FDIC, the OCC, the OTS, and the National Credit Union Administration) issued guidance for banks offering Internet-based financial services. This guidance describes enhanced methods regulators expect banks to use when authenticating the identity of customers using online products and services. Financial institutions are expected to comply by year-end 2006.
Relationship Manager Program (FIL-98-2005, October 6, 2005)	The FDIC has implemented the Relationship Manager Program (RMP) for all FDIC-supervised financial institutions. The RMP is designed to strengthen lines of communication between bankers and the FDIC, as well as improve the coordination, continuity, and effectiveness of FDIC supervision.
Revised Plan for Implementation of Basel II Framework (PR-98-2005, September 30, 2005)	The four Federal banking agencies announced revised plans for the U.S. implementation of Basel II. The agencies plan to introduce in a notice of proposed rulemaking additional prudential safeguards to address concerns raised by the Fourth Quantitative Impact Study.
Implementation of the Central Data Repository (FIL-93-2005, September 15, 2005)	The FDIC, OCC, and Board of Governors of the Federal Reserve System will implement the Central Data Repository (CDR) to process the Reports of Condition and Income (Call Reports) beginning with third quarter 2005. The CDR will require banks to validate their Call Report data before they will be accepted. The new CDR system will be the only method available for banks to submit Call Reports. Banks were advised via FIL-55-2005, June 29, 2005, and PR-59-2005, June 30, 2005, of the need to enroll in the CDR to file their Call Report data via the new system.

Regulatory and Supervisory Roundup

continued from pg. 33

Subject	Summary
Residential Tract Development Lending Frequently Asked Questions (FIL-90-2005, September 8, 2005)	The Federal financial institution regulatory agencies issued guidance on residential tract development lending to assist institutions in complying with the agencies' appraisal and real estate lending requirements.
List of Distressed and Underserved Nonmetropolitan Middle-Income Geographies (PR-82-2005, August 30, 2005)	The Board of Governors of the Federal Reserve System, the FDIC, and the OCC announced the availability of the list of distressed and underserved nonmetropolitan middle-income geographies in which bank revitalization or stabilization activities will receive Community Reinvestment Act (CRA) consideration as "community development," pursuant to the revised CRA rules issued by the agencies on August 2, 2005. The list is available at www.ffiec.gov/cra.
New Information Technology Examination Procedures (FIL-81-2005, August 18, 2005)	The FDIC has updated its risk-focused information technology (IT) examination procedures for FDIC-supervised financial institutions. The IT-Risk Management Program examination procedures apply to all FDIC-supervised banks, regardless of size, technical complexity, or prior examination rating.
Guidance on Implementing a Fraud Hotline (FIL-80-2005, August 16, 2005)	The FDIC is providing guidance to financial institutions on implementing a fraud hotline to minimize potential and actual fraud risks as part of a bank's governance and enterprise risk management program.
Recommendations Sought for Reducing Regulatory Burden (*Federal Register,* Vol. 70, No. 154, Page 46779, August 11, 2005, and FIL-82-2005, August 19, 2005)	The Federal financial institution regulatory agencies asked for recommendations on how to reduce regulatory burden in rules related to Banking Operations; Directors, Officers, and Employees; and Rules of Procedure. Comments were due by November 9, 2005.
Proposed New Rule on Insurability of Funds Underlying Stored Value Cards (*Federal Register,* Vol. 70, No. 151, Page 45571, August 8, 2005, and FIL-83-2005, August 22, 2005)	The FDIC proposed a new rule on the insurability of funds subject to transfer or withdrawal through the use of stored value cards and other nontraditional access devices, such as computers. This proposed rule replaces the proposed rule issued in April 2004. Comments were due by November 7, 2005.
Bank Secrecy Act Anti-Money Laundering Examination InfoBase (FIL-76-2005, August 9, 2005)	The FFIEC introduced its Bank Secrecy Act/Anti-Money Laundering Examination (BSA/AML) InfoBase, an automated tool for examiners and the industry. This automated tool features the FFIEC's BSA/AML Examination Manual, examination procedures and appendixes, frequently asked questions, and links to resources that may be helpful in understanding BSA/AML requirements and examination expectations. The InfoBase is available at www.ffiec.gov/bsa_aml_infobase.
Proposed Rules on Post-Employment Restrictions for Senior Examiners (PR-74-2005, August 4, 2005, and *Federal Register,* Vol. 70, No. 150, Page 45323, August 5, 2005)	The Federal banking agencies issued proposed rules to implement a special post-employment restriction for one year on certain senior examiners employed by an agency or Federal Reserve Bank. Comments were due by October 4, 2005.

Subject	Summary
Supervisory Guidance on the Eligibility of Asset-Backed Commercial Paper Liquidity Facilities and the Resulting Risk (FIL-74-2005, August 4, 2005)	The Federal financial institution regulatory agencies issued supervisory guidance clarifying the application of the asset quality test for liquidity facilities that provide support to an asset-backed commercial paper (ABCP) program. This guidance supplements the "Final Rule on Capital Requirements for Asset-Backed Commercial Paper Programs" issued July 28, 2004 (see FIL-87-2004).
Final Community Reinvestment Act Rules (*Federal Register*, Vol. 70, No. 147, Page 44256, August 2, 2005, and FIL-79-2005, August 9, 2005)	The FDIC, OCC, and the Board of Governors of the Federal Reserve System issued final CRA rules intended to reduce regulatory burden on community banks while making CRA evaluations more effective in encouraging banks to meet community development needs. The final rules raise the small-bank asset threshold to less than $1 billion without regard to holding company affiliation. The new rules also reduce data collection and reporting burden for "intermediate small banks" (banks with assets of at least $250 million but less than $1 billion). The final rules took effect September 1, 2005.
Proposed Amendment to Part 363 - Annual Independent Audits and Reporting Requirements (*Federal Register,* Vol. 70, No. 147, Page 44293, and FIL-72-2005, August 2, 2005)	The FDIC is proposing to raise the asset threshold from $500 million to $1 billion for requirements relating to internal control assessments and reports by management and external auditors, and the requirement that members of the audit committee, who must be outside directors, be independent of management. Comments were due by September 16, 2005.
Guidance on Risks of Voice Over Internet Protocol (VoIP) (FIL-69-2005, July 27, 2005)	The FDIC issued guidance to financial institutions on the security risks associated with voice over Internet protocol (VoIP). VoIP refers to the delivery of traditional telephone voice communications over the Internet.
Guidance on Mitigating Risks From Spyware (FIL-66-2005, July 22, 2005)	The FDIC issued guidance recommending an effective spyware prevention and detection program based on an institution's risk profile. Spyware is software that collects information without the prior knowledge or informed consent of the data's owner. This guidance discusses the risks associated with spyware from both a bank and consumer perspective and provides recommendations to mitigate these risks.
Guidance on How Financial Institutions Can Protect Against "Pharming" Attacks (FIL-64-2005, July 18, 2005)	The FDIC issued guidance describing the practice of "pharming," how it occurs, and potential preventive approaches. Financial institutions offering Internet banking should assess potential threats posed by pharming attacks and protect Internet domain names, which — if compromised — can heighten risks to the institutions.
Identity Theft Study Supplement on "Account-Hijacking" Identity Theft (FIL-59-2005, July 5, 2005)	The FDIC issued a supplement to its December 14, 2004, study on account-hijacking identity theft (see FIL-132-2004). The supplement reviews and responds to public comments on the original study, surveys recent trends in identity theft and account hijacking, and discusses authentication technologies.
Bank Secrecy Act/Anti-Money Laundering Examination Manual (FIL-56-2005, June 30, 2005)	The FFIEC has issued the ***BSA/AML Examination Manual***. The Manual, which BSA/AML examiners began using during third quarter 2005, is available at www.ffiec.gov/press/pr063005.htm.

Regulatory and Supervisory Roundup

continued from pg. 35

Subject	Summary
Fair Credit Reporting Act Medical Information Interim Final Rules (*Federal Register,* Vol. 70, No. 111, Page 33996, June 10, 2005, and FIL-51-2005, June 16, 2005)	The Federal financial institution regulatory agencies issued interim final rules under the Fair Credit Reporting Act that create exceptions to the statutory prohibition against obtaining or using medical information in connection with credit eligibility determinations. The interim final rules also address the sharing of medical information among affiliates. The interim final rules will take effect on March 7, 2006.
Guidance on Developing an Effective Pre-employment Background Screening Process (FIL-46-2005, June 1, 2005)	The FDIC's guidance can be an effective risk management tool that provides management with a degree of certainty that the information provided in the background screening is accurate and the applicant does not have a criminal background.
Credit Risk Management Guidance for Home Equity Lending (FIL-45-2005, May 24, 2005)	The Federal financial institution regulatory agencies issued guidance promoting sound risk management practices for home equity lines of credit and loans. In some cases, the agencies have found that credit risk management practices for home equity lending have not kept pace with the product's rapid growth and eased underwriting standards.
Unsafe and Unsound Use of Limitation of Liability Provisions in External Audit Engagement Letters (FIL-41-2005, and *Federal Register,* Vol. 70, No. 89, Page 24576, May 10, 2005)	The Federal financial institution regulatory agencies are seeking public comment on a proposed advisory that alerts financial institutions' boards of directors, audit committees, management, and external auditors to the safety and soundness implications of provisions that limit the external auditor's liability in a financial statement audit. Comments were due by June 9, 2005.
International Banking Final Rule (FIL-40-2005, May 6, 2005 and *Federal Register,* Vol. 70, No 65, Page 17550, April 6, 2005)	The FDIC has adopted various amendments and revisions to its international banking rules, effective July 1, 2005. The final rule amends Parts 303, 325, and 327 relating to international banking and revises Part 347, Subparts A and B.
Accounting and Reporting for Commitments to Originate and Sell Mortgage Loans (FIL-39-2005, May 3, 2005)	The Federal financial institution regulatory agencies issued guidance on the application of Statement of Financial Accounting Standards No. 133, ***Accounting for Derivative Instruments and Hedging Activities***, as amended, to mortgage loan commitments. The guidance also addresses related regulatory reporting requirements and valuation considerations.

Subscription Form

To obtain a subscription to ***Supervisory Insights***, please print or type the following information:

Institution Name _____

Contact Person _____

Telephone _____

Street Address _____

City, State, Zip Code _____

Please fax or mail this order form to:

FDIC Public Information Center
801 17th Street, N.W., Room 100
Washington, D.C. 20434
Fax Number (202) 416-2076

Subscription requests also may be placed by calling 1-877-ASK-FDIC or 1-877-275-3342.

FDIC

Federal Deposit Insurance Corporation
Washington, DC 20429-9990

OFFICIAL BUSINESS
PENALTY FOR PRIVATE USE, $300

PRESORTED
STANDARD
MAIL
Postage &
Fees Paid
FDIC
Permit No. G-36