
Model Risk Management Framework
and Related Regulatory Guidance

April 2012

Prepared by:

David J. Green, Ph.D., CFA
Managing Director

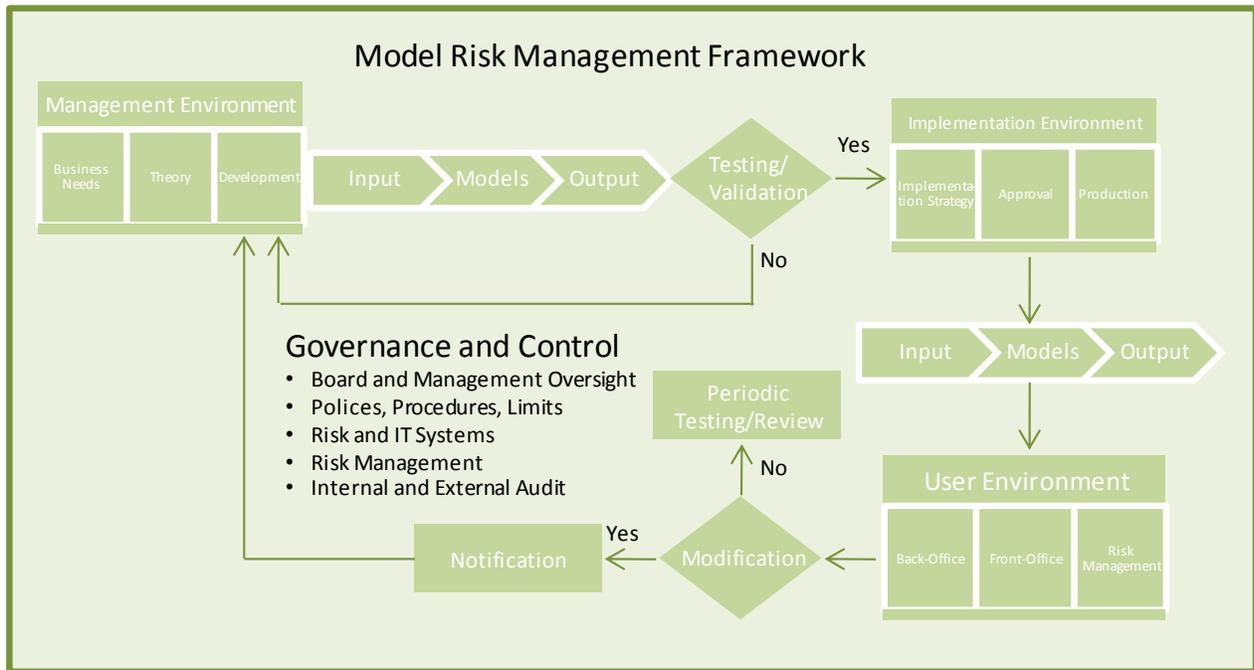


Model Risk Management Framework and Related Regulatory Guidance

Contents

Model Risk Management Framework.....	1
Summary of OCC Bulletin 2011-12 Model Risk Management	11
Summary of OCC Bulletin 2000-16 Risk Modeling: Model Validation	18
Summary of "Model Governance," FDIC	22
Summary of FFIEC Guidelines on Interest Rate Risk Management	29
Angel Oak Advisory.....	31

Model Risk Management Framework



In this piece, we will briefly expound upon Angel Oak's overall view of the Model Risk Management Framework, where we address a few obvious questions:

- Why validate a model?
- What is model risk?
- How can validation be used to mitigate model risk?

Regulatory Perspective

Regulated entities such as commercial banks and thrifts are required to validate models that are used in a variety of business functions. These models can take the form of "black-box" third party models, custom implementations of third party applications, or internally developed tools, including Excel spreadsheets. (See inset on next page for areas/business functions where model risk can be found.) The scope of regulatory guidance has grown as the use of computerized financial models has expanded rapidly into an increasing number of business functions. Some of the earliest guidance is found in the Joint Interagency Statement on Interest Rate

Risk Management in 1996, which emphasized the importance of an adequate risk management process that includes the capability to identify, measure, and monitor risk. The guidance describes senior management's responsibility to provide an appropriate system of internal controls that will ensure the integrity of the overall risk management process as well as oversight mechanisms to ensure the integrity of information used by the board and senior management in overseeing compliance with policies and limits. Organizations are required to demonstrate:¹

- The appropriateness of the bank's risk measurement system given the nature, scope and complexity of its activities.
- The accuracy and completeness of the data inputs into the risk measurement system.
- The reasonableness and validity of scenarios used in the risk measurement system.
- The validity of the risk measurement calculations, often tested by comparing actual versus forecasted results.

Examples of Model Risk Exposures:

- ***Asset/Liability Management:***
 - *NII Simulation*
 - *EVE/NPV*
 - *Core Deposit Behaviors*
 - *Loan Prepayments*
- ***Credit:***
 - *Loan Pricing*
 - *Scoring Methodology*
 - *LLL Reserve/Provision*
 - *Risk Limit Scorecards*
- ***Trading/Portfolio Management:***
 - *VAR limit measurement/hedging*
 - *Mortgage & ABS Pricing*
 - *Derivative Pricing*

Compliance with these requirements ultimately necessitates a review and validation by an independent source such as an internal risk control unit of the bank or outside consultants or auditors.

In 2000, the Office of the Comptroller of the Currency (OCC) acknowledged the increased reliance on computer-based financial models in such areas as enterprise-wide risk management, economic and regulatory capital allocation, whole bank credit risk, fiduciary asset management, and internal profitability measurement. They published guidance that outlined specific model validation principles as well as expectations for a sound model validation.² This regulatory guidance speaks to three core components of the modeling process: Inputs, Models, and Output. The OCC clearly states that "errors in any of these components can cause the model's information to be meaningless or misleading." They specifically recognize that many models require considerable

¹ The Joint Interagency Statement was published in Federal Register, Vol. 61, No. 124, June 26, 1996.

² See Appendix C for summary of OCC 2000-16 Risk Modeling: Model Validation.

judgment and expertise in their construction and use, facts that may challenge the transparency and correctness of key assumptions. In several instances, they have observed that decision makers relied upon erroneous construction or use which led to “serious consequences for their bank’s reputation and profitability.” In addition, the OCC has noted the *potential* for large losses associated with model errors. These problems and challenges are collectively viewed under the heading of model risk. In addressing this risk, the guidance goes on to state that “model validation not only increases the reliability of a model, but also promotes improvements and a clear understanding of a model’s strengths and weaknesses among management and user groups.” In 2011, this guidance was revised and expanded to emphasize the importance of governance and controls in the model risk management process.³ Governance includes the use of policies, procedures and oversight relating to the development, implementation and use of models. This guidance has been adopted by all major bank regulatory authorities.

“...using unvalidated models to manage risks to the bank is potentially an unsafe and unsound practice. Even where the risk is not particularly material, the reliance on unvalidated models can be a poor business practice.”

- OCC 2000-16

Other regulators have weighed in as well. The Basel Committee on Bank Supervision provided an internationally harmonized statement in 2004 that noted the importance of rigorous model validation as a component of the Pillar II requirements for ensuring capital adequacy.⁴ The FDIC published a statement in 2005 which discusses the use of models in banking and describes a broad conceptual framework for model governance.⁵ In addition, the article suggests possible areas of examiner review when evaluating the adequacy of an institution's model oversight, controls and validation practices. In its oversight of the Federal Home Loan Banks, the Federal Housing Finance Agency provided guidance in 2009 requiring model validation to include the following key areas of assessment:⁶

- Policies, procedures, and documentation;
- Data and assumptions: external and internal data aggregation and integration;

³ See Appendix B for summary of OCC 2011-12 Model Risk Management.

⁴ See Basel II: International Convergence of Capital Measurement and Capital Standards: a revised Framework, June 2004 and subsequent revision in November 2005; available as comprehensive version in June 2006.

⁵ See Appendix D for FDIC Statement on Model Governance; published in Supervisory Insights, Winter 2005, Vol. 2, Issue 2.

⁶ See Federal Housing Finance Agency, Advisory Bulletin 2009-AB-03, December 2009.

- Model theory: code and mathematics;
- Model output: reporting and controls;
- Back testing and benchmarking processes.

While the FHFA guidance does not apply directly to banks and thrifts, it is indicative of a more comprehensive view of model validation and is representative of best practices for any institution relying upon financial models.

More recently, the Federal Financial Institutions Examination Council (FFIEC) released an advisory in 2010 reiterating supervisory expectations for sound practices for managing interest rate risk.⁷ This advisory reiterates the importance of model validation for both internally developed as well as vendor-based models and further emphasizes an expanded view on risk that goes beyond interest rate volatility to assess the impact of liquidity, credit, and other risk factors.

In summary, we see an evolution of thought from a host of regulatory authorities that acknowledges:

- 1) the rapidly expanding use of models into a variety of business functions,
- 2) that model validation is a critical component in the model risk management process, and
- 3) the model validation process must necessarily incorporate a view beyond the mere technical details of the model calculations.

Best Practices

While these advisories and guidelines have been applied primarily to regulated financial institutions, many of their key components have been adopted as best practices by many different types of non-bank firms, especially those that are exposed to significant amounts of market or credit risk that must be monitored and managed with sophisticated models. These would include money managers, hedge funds and insurance companies to name just a few. Even though there is broad applicability of the basic principles, there is no single “silver-bullet” solution for the conduct of model validation that can be developed from these guidelines. Effective model validation requires an assessment of the unique risk exposures that each organization faces and a practical experience-driven grasp of the best practices that have evolved to supplement basic regulatory expectations. Organizational nuances including size, complexity, staffing and accountabilities are sufficiently idiosyncratic to make any company’s model risk management process unique. In assessing the efficacy of a company’s model risk management process, each of these nuances must be addressed.

⁷ See Appendix E for summary of January, 2010 FFIEC Advisory.

These regulatory guidelines and industry best practices are critical elements that must be embedded in an organization's governance policy and control procedures. Policies and procedures must address resource requirements and alignment in order to ensure consistent and disciplined model use and validation across a firm. Decision makers must clearly articulate minimum expectations relating to how model risk management is accomplished. The validation process for model use in any functional area, whether performed by central audit or an internal/external model validation team, should be consistent with the Company's corporate standards articulated in the overall governance policy.

Validation policies need not be highly prescriptive as to the actual validation steps (as they are generally designed to address a broad range of models and applications), but they should require that model owners clearly document their model with particular emphasis on highlighting key assumptions and articulating necessary inputs. This documentation will serve as a roadmap for whoever is validating the modeling process. Any validation should clearly define the scope of the model testing. This documentation will serve to identify areas that require further testing or conditions of use which, if changed, will require additional validation. Further, access to models and change controls should be governed in a manner consistent with the Company's IT security standards.

Internal Audit should play a prominent and active role in monitoring consistency with corporate standards over time and keep senior management informed of compliance. They should be able to verify that specific policies governing model development and validation are in place and are consistent with overall model governance policy. While Internal Audit may not have the technical or quantitative expertise to perform validations, they should have sufficient expertise to determine if the model validation process is effective.

Model Risk

Model risk can arise from poor assumptions, inputs, calibration or implementation. Weaknesses in any of these areas can impair reliance on model results. In addition, we believe that how a model is developed and managed impacts its susceptibility to one form of model risk relative to another. For example, IRR models, given the broad range of required components, are particularly complex to begin with and are subject to constant adjustment and calibration. This inherent complexity and dynamic nature provides considerable room for the introduction of errors that begin with model design, such as the inconsistent application of assumptions and modeling techniques across business lines and products, and continue on through model use and maintenance. The control processes around the management of inputs, construction, use and reporting are central to a well-run modeling process. The larger and more complex an organization, the more exposure a company has to model risk.

In addition to the purely technical elements of inputs, calculations and output, the use and interpretation of results is a source of model risk. Many financial models are forward looking in nature yet are often calibrated to historically observed behaviors. While such forward looking risk measures should be “back-tested,” the notion that history does not necessarily repeat itself should be effectively captured in the presentation of findings and recommendations. Examples of such risk can be found in the use of loan and credit card prepayment functions and core deposit behaviors. Recent legislative changes, the drastic reduction in home prices, as well as the tightening of credit are key behavioral drivers that limit the usefulness of pure historical studies. While such studies will serve as a useful guide, forward looking models should capture and expose the uncertainty associated with key behavioral assumptions. Findings should include clear disclosures and sensitivity analysis on key assumptions. Transparency is a critical component of the reporting process.

While most instances of modeling error remain relatively innocuous or simply go unreported, in several well-known cases trading firms have incurred substantial losses resulting from the use of untested or improperly validated models.⁸ In a more recent case, lack of effective governance resulted in severe fines for a company.⁹ In addition to the monetary penalties, the company, an asset manager, suffered reputational repercussions in the form of fund outflows. Given these examples, it is incumbent upon any organization to think critically about its exposure to model risk.

Model Validation

While any model validation will incorporate an analysis of a model’s inputs, computational engine, and outputs, the (internal aspect of the) model validation process should optimally begin during the model creation process in order to ensure that all sources of model risks are appropriately identified and addressed. Additionally, any changes to a model’s design or enhancements to accommodate new products, behavioral elements or reports should be considered in light of existing assumptions and limitations around use and any updates that may need to occur in the validation process. With regard to a governing model validation policy that is applicable across an entire organization, bank examiners and auditors would be expected to determine whether the testing

⁸ In 1997, Bank of Tokyo/Mitsubishi reported an \$83 million after-tax loss related to errors with a model used to value interest rates swaps and options. In the same year, NatWest Capital Markets reported a \$138 million charge because of poorly constructed models for interest rate options and swaptions. See *Derivatives Strategy*, June 1997.

⁹ On February 3, 2011, the SEC charged three AXA Rosenberg entities with concealing errors in a quantitative investment model. The firm had to remit \$217 million to harmed clients and a \$25 million penalty. The SEC additionally charged that one of the entities with “failing to adopt and implement compliance policies and procedures to ensure that the model would work as intended.”

criteria have been applied consistently across models that pose similar risks. Any validation should be regarded in this broader context.

As with model developers, model validators should ensure that the results of their own model testing are well documented. At minimum, validation documentation should contain a scope that clearly articulates aspects of the model reviewed, highlights potential model deficiencies, the range of market conditions over which these deficiencies could manifest themselves and whether model reserves are warranted. An assessment of input availability for the purpose of calibration should also be included in the validation document and the bank should verify that the model is implemented in a manner consistent with its testing environment and its intended use.

The rigor of model testing involves an assessment of how effective the testing process is at identifying the vulnerability of models to poor assumptions, inputs, calibration or implementation as well as how consistent testing is across models that pose similar risks. The testing process should be tailored to the complexity of the model and involve a combination of benchmarking, sensitivity analysis and, where possible, back-testing. To ensure that model testing is sufficiently rigorous and appropriately tailored to the complexity of the model in accordance with supervisory expectations, examiners and auditors are likely to raise the following questions:

- Does model validation documentation clearly articulate the scope of the model review?
- Does model validation documentation clearly identify model assumptions and whether they are consistent with industry practice and the academic literature?
- To what extent does the bank use benchmarking, sensitivity analysis and back-testing to assess model adequacy?
- To what extent are model deficiencies highlighted in the validation documentation?
- Does the validation documentation include an assessment as to whether reserves are required?
- Does the validation documentation include an assessment of input availability?
- How does the bank ensure that the model is tested in a manner consistent with how it is to be implemented and its intended use?

To assess the rigor of testing and ensure that model deficiencies are identified, auditors should:

- Sample validation documents for models used for products, positions or limits that pose material risk;
- Identify the scope of review, sources of model risk investigated and the approval decision;

- Ensure that sampled documents cover the range of product and model complexity at the bank to determine whether validation techniques are appropriately tailored to the sophistication of the model; and
- Discuss the sample validation documents with the validation staff, which should be able to justify the level and rigor of review applied to the model.

In the case of complex balance sheet and IRR management models, many companies utilize third-party vendor models. In addition, they rely upon significant assistance from the vendor for implementation assistance. While implementation consultants may be very familiar with the software's many complex features, they are not likely to be familiar with many of the company's products and their behavioral nuances. In the desire to expedite the installation process, assumptions may be made regarding product behaviors. These behavioral assumptions will ultimately need to be properly substantiated and reconciled to the company's historical or projected experience. A company must ensure that the resulting model is not simply a "black box" that is presumed to work correctly. The model validation should ensure proper implementation and use of such third party models.

Banks may not necessarily validate models purchased from vendors that they believe to be "industry standard". The bank should perform a validation regardless of whether others are running the same vendor system because it is possible that each has different versions or releases and therefore functionality. As a result, different banks may have different software errors (bugs) or bug fixes that might be present in one version but not the other. Moreover, assuming that models have been appropriately validated in a system used by others effectively runs the risk that no one actually does a thorough validation of such models.

It is worth noting that, in practice, validation of vendor systems focuses more on input availability and implementation issues rather than the theoretical specifications or the mathematical correctness of the model. In most instances, this emphasis is appropriate because the mathematics underlying the model is fairly standard and well understood to be theoretically correct. With that in mind, to the extent that the mathematics is non-standard or not well established in academic circles, banks would be expected to validate the mathematical specifications of the model.

Model risk can also arise in an externally developed model when it is used for a purpose different from its intended purpose. Typically, this occurs because management lacks sufficient understanding of model assumptions, data needs or system requirements. In addition to ongoing oversight by internal audit, a comprehensive validation should address model purpose and intended use.

In many cases, institutions rely on external auditors or consultants to perform model validations. It is important that the bank be actively involved in setting the scope of the validation to ensure that material sources of model risk are assessed. Material sources of model risk may not be assessed because the scope is too narrow or the external auditors or consultants do not understand the validation requirements of the institution. As a result, it is important for the bank to work with external auditors and consultants so that they are aware of validation policies and can perform their review in accordance with those policies.

To assess whether externally developed models are validated in accordance with supervisory expectations and business best practices, key questions that should be asked include:

- To what extent does the bank rely on external model development?
- What due diligence has the bank performed to ensure vendor support is adequate given its needs?
- How has the bank assessed its risk in the event that the vendor fails?
- To what extent does the bank validate externally developed models?
- If the bank validates externally developed models, what does validation entail?
- Is vendor documentation sufficiently comprehensive for the bank to perform its own validation?
- What training if any does the vendor provide?
- To what extent does the bank rely on external consultants or auditors?
- How involved is the bank in defining the scope of the external consultant's or auditor's review?

To evaluate a bank's use of third-party models and determine whether they expose a bank to excessive model risk, auditors or examiners should:

- Discuss with management why it has chosen the particular vendor;
- Review vendor documentation to assess its comprehensiveness;
- Review validation performed by Internal Audit;
- Transaction test sample external consultant or audit reviews to determine whether material sources of model risk have been addressed; and
- Evaluate contingency plans in the event of vendor failure.

Summary

Angel Oak is able to provide your company a Comprehensive Strategic and Tactical Risk Model Validation in consideration of the entire Model Risk Management Framework as described above. More limited forms of model validation are available. These may be acceptable as long as the entire Model Risk Management Framework has been previously addressed or is handled by appropriately qualified Internal Audit or Model Validation resources.

Summary of OCC Bulletin 2011-12 Model Risk Management

This guidance revises and expands important regulatory considerations for model risk management. It was adopted by all bank regulatory authorities.

Key Excerpts

The guidance recognizes the expanded use of models for a broad range of activities, including the measurement and management of risk, determination of valuations and capital adequacy as well as the management and safeguarding of client assets. The ambitious scope of model use has occurred both in response to changing regulatory requirements, for instance in relation to the determination of Basel capital and stress testing requirements, but also to the move toward more data-driven decision making processes. While the use of well-structured models can improve decision-making processes, their use comes with certain costs that must be recognized. Aside from the direct costs of building and maintaining complex financial models, the indirect cost, or risk associated with relying on models that are incorrect or misused, must be managed.

The guidance emphasizes that while a rigorous model validation process plays a critical role in model risk management, sound development, implementation and use of models are also key elements in the model management process. These latter items all fall under a comprehensive notion of model governance. Governance also includes board and senior management oversight, policies and procedures, controls and compliance and an appropriate incentive and organizational structure.

Overview of Model Risk Management

A model consists of three components:

- 1) Information Input
- 2) Processing/Transformational engine
- 3) Reporting and output

Models are simplified representations of real-world phenomena. Given that simplifications and assumptions naturally introduce error into the model, it is important to understand a model's capabilities and limitations. Model risk is defined as the potential for adverse consequences from decisions based on incorrect or misused model outputs and reports. Model risk occurs because models may have certain fundamental errors. Such errors can occur anywhere in between design and implementation. Specifically, simplifications or approximations associated

with modeling complex processes can compromise model integrity and reliability of outputs. Additionally, errors in inputs or assumptions can lead to model errors.

Models may also be used incorrectly or inappropriately. While a model may be well-constructed for its intended use, in time models are often tasked to address certain problems for which they were not intended. Banks often do this unintentionally. Products and behaviors change and may render key model assumptions invalid. Modeling and development personnel experience turnover and may no longer be in a position to clarify intended uses and limitations.

Model risk should be managed similarly to other types of risk. Risk sources should be identified and managed according to their severity and magnitude. Banks should consider model risk from individual models and in the aggregate. Aggregate risk is affected by the interaction and dependencies among models. Models may rely on common assumptions, data or methodologies, errors in which may impact multiple models across an organization.

A guiding principle for managing model risk is "effective challenge" of models, that is, critical analysis by objective, informed parties who can identify model limitations and assumptions and produce appropriate changes. Effective challenge depends on a combination of incentives, competence and influence.

For institutions where model output has a material impact on business decisions and where model failure can be particularly harmful to the bank's financial condition, the model risk management framework should be more extensive and rigorous. The framework consists of three primary elements:

- 1) Robust controls around model development, implementation and use.
- 2) A sound model validation process.
- 3) Effective Governance

Model Development, Implementation, and Use

Model risk management begins with disciplined and knowledgeable development processes. Such processes need to be designed by experienced developers, who have relevant training and experience, technical knowledge and can provide guidance on informed business use. Model development and implementation often rely upon subjective judgement. The subjective nature of the exercise elevates the importance of sound business judgement.

Model development should begin with a clear statement of purpose to ensure that model development is properly aligned with the intended uses. Design, theory, and logic of the model should be well documented and be consistent with sound industry practice. Developers should ensure that the components work as intended, are appropriate for the intended business purpose, and are conceptually sound and mathematically and statistically correct. Any data that are used to develop the model should be suitable for the intended purpose and well-documented. Any assumptions that are utilized should be tracked and analyzed so that users are aware of any limitations.

Model development should contain an extensive testing component. Model testing includes checking the model's accuracy, demonstrating that the model is robust and stable, assessing potential limitations, and evaluating the model's behavior over a range of input values. Situations and assumptions should be analyzed to determine where the model performs poorly or becomes unreliable. Extreme values for inputs or other stress tests should be used to determine how the model performs under unexpected circumstances. Testing activities should be thoroughly documented.

Model use generates an additional opportunity to obtain feedback on the effectiveness of the design and implementation of the model. The quality and extent of feedback will depend upon how model results affect business decisions. If model results negatively affect business decisions and outcomes, model developers are forced to explain and justify the assumptions and design of the model. If model results do not affect business decisions, feedback may be limited or do little to instigate better development. The nature and motivation beyond user input needs to be thoroughly understood. Feedback from an independent third party provides a valuable supplement to user feedback.

Reports that are designed for end-users should be comprehensive and clear, providing a range of input-value scenarios and assumption values in order to highlight the model's accuracy, robustness, stability and limitations. Using a range of output values can be a useful way to demonstrate model uncertainty and avoid spurious precision. This can also be accomplished by adjusting model inputs or calculations to produce more severe model outcomes. In either case, models should be used conservatively and in a way that recognizes the inherent uncertainty and inaccuracy in the modeling process.

Model Validation Process

Model validation is the set of processes and activities intended to verify that models are performing as expected, in line with their design objectives and business uses. Effective validation helps ensure that models are sound. It also identifies potential limitations and assumptions, and assesses their possible impact. As with other

aspects of effective challenge, model validation should be performed by staff with appropriate incentives, competence, and influence.

Input, processing and output components should be validated, whether models are developed in-house or obtained from a third-party vendor. Validation should be performed by individuals that are independent of those responsible for development and implementation. Additionally, validation personnel should not have a stake in whether a model is deemed valid or not. Overall, the quality of the model validation process is judged by the manner in which models are subject to critical review. This can be determined by evaluating the extent and clarity of documentation, the issues identified by objective parties and the actions taken by management to address model issues. Compensation, performance evaluations and corporate culture play an important role in establishing support for independent and objective thinking.

Validation staff should have requisite knowledge, skills and expertise. Staff should also have a significant degree of familiarity with the line of business using the model and the model's intended use. Validation staff should also have authority to challenge developers and users of models and have the ability to appropriately elevate their findings.

If significant deficiencies are noted as a result of the validation process, use of the model should not be allowed or should be permitted only under very tight constraints until those issues are resolved. Validation activities should remain ongoing to track model limitations and identify new ones. Banks should conduct a periodic review, at least annually, of each model to determine whether it is working as intended and if the existing validation activities are sufficient.

Effective model validation helps reduce model risk by identifying model errors, corrective actions, and appropriate use. An effective validation framework should include three core elements:

- 1) Evaluation of conceptual soundness, including developmental evidence
- 2) Ongoing monitoring, including process verification and benchmarking
- 3) Outcomes analysis, including back-testing

The first element involves assessing the quality of the model design and construction. It entails a review of documentation and empirical evidence supporting the methods used and variables selected for the model. A sound development process will produce documented evidence in support of all model choices, including the overall theoretical construction, key assumptions, data, and specific mathematical calculations. Stress testing and sensitivity analysis should be utilized to analyze the range of outcomes to ensure they fall within expected

levels and that the model is robust. Any qualitative information and judgement used in model development should be evaluated for appropriateness and should be supported and well-documented.

The second element, ongoing monitoring, confirms that the model is appropriately implemented and is being used and is performing as intended. Ongoing monitoring is essential to evaluate whether changes in products, exposures, activities, clients, or market conditions necessitate adjustment, redevelopment, or replacement of the model and to verify that any extension of the model beyond its original scope is valid. This element should include process verification and benchmarking. Benchmark models should be rigorous and benchmark data should be accurate and complete to ensure a reasonable comparison.

The third element of model validation, outcomes analysis, provides a comparison of model outputs to corresponding actual outcomes. The precise nature of the comparison depends on the objectives of a model, and might include an assessment of the accuracy of estimates or forecasts, an evaluation of rank-ordering ability, or other appropriate tests. In all cases, such comparisons help to evaluate model performance, by establishing expected ranges for those actual outcomes in relation to the intended objectives and assessing the reasons for observed variation between the two. Outcomes analysis should be conducted on an ongoing basis. Back-testing is one form of outcomes analysis; specifically, it involves the comparison of actual outcomes with model forecasts. The objective of the analysis is to determine whether differences stem from the omission of material factors from the model, whether they arise from errors with regard to other aspects of model specification such as interaction terms or assumptions of linearity, or whether they are purely random and thus consistent with acceptable model performance.

Regulators acknowledge that data, assumptions and models may be sourced from third party vendors. This presents unique challenges for model validation as there are likely proprietary aspects to this information. Nonetheless, vendor products should be included in the bank's broader model risk management framework and should follow similar principles that are applied to in-house models. Banks should expect vendors to conduct ongoing performance monitoring and outcomes analysis, with disclosure to their clients, and to make appropriate modifications and updates over time. Banks are expected to validate their own use of vendor products. External models may not allow full access to computer coding and implementation details, so the bank may have to rely more on sensitivity analysis and benchmarking. Vendor models are often designed to provide a range of capabilities and so may need to be customized by a bank for its particular circumstances. A bank's customization choices should be documented and justified as part of validation.

Governance, Policies and Controls

Developing and maintaining strong governance, policies, and controls over the model risk management framework is fundamentally important to its effectiveness. Even if model development, implementation, use, and validation are satisfactory, a weak governance function will reduce the effectiveness of overall model risk management. A strong governance framework provides explicit support and structure to risk management functions through policies defining relevant risk management activities, procedures that implement those policies, allocation of resources, and mechanisms for evaluating whether policies and procedures are being carried out as specified. Notably, the extent and sophistication of a bank's governance function is expected to align with the extent and sophistication of model usage.

Model risk governance begins with the board of directors and executive management as these parties are responsible for establishing and enforcing bank-wide risk management policies. Governance should include standards for model development, implementation, use and validation. Senior management is responsible for establishing adequate policies and procedures and ensuring compliance with model risk management objectives.

Banks are expected to formalize board-approved policies and procedures to manage model risk management activities. All aspects of model risk management should be covered by suitable policies, including model and model risk definitions, assessment of model risk, acceptable practices for model development, implementation, and use, appropriate model validation activities and governance and controls over the model risk management process.

While there are several ways in which banks can assign the responsibilities associated with risk management roles, it is important that reporting lines and incentives be clear, with potential conflicts of interest identified and addressed. Business units are generally responsible for the model risk associated with their business strategies. The role of model owner involves ultimate accountability for model use and performance within the framework set by bank policies and procedures. The model owner should also ensure that models in use have undergone appropriate validation and approval processes, promptly identify new or changed models, and provide all necessary information for validation activities. Control staff should have the authority to restrict the use of models and monitor any limits on model usage.

A bank's internal audit function should assess the overall effectiveness of the model risk management framework, including the framework's ability to address both types of model risk (fundamental errors at any point between design and implementation and incorrect or inappropriate model use), for individual models and in the aggregate. Internal audit's role is to evaluate whether model risk management is comprehensive, rigorous and

effective. Additionally, internal audit should perform assessments of supporting operational systems and evaluate the reliability of data used by models. Internal audit also has an important role in ensuring that validation work is conducted properly and that appropriate effective challenge is being carried out. It should evaluate the objectivity, competence, and organizational standing of the key validation participants, with the ultimate goal of ascertaining whether those participants have the right incentives to discover and report deficiencies. Internal audit should review validation activities conducted by internal and external parties with the same rigor to see if those activities are being conducted in accordance with this guidance.

External resources may be appropriately utilized in order to bring necessary expertise to the model risk management process, such as model validation and review. External resources can bring added knowledge and another level of critical and effective challenge.

Banks should maintain a comprehensive set of information for models implemented for use, under development for implementation, or recently retired. A specific party should also be charged with maintaining a firm-wide inventory of all models, which should assist a bank in evaluating its model risk in the aggregate. The inventory should describe the purpose and products for which the model is designed, actual or expected usage and any restrictions on use.

Without adequate documentation, model risk assessment and management will be ineffective. Documentation of model development and validation should be sufficiently detailed so that parties unfamiliar with a model can understand how the model operates, its limitations, and its key assumptions. Documentation provides for continuity of operations, makes compliance with policy transparent, and helps track recommendations, responses, and exceptions. Documentation takes time and effort, and model developers and users who know the models well may not appreciate its value. Banks should therefore provide incentives to produce effective and complete model documentation.

Validation reports should articulate model aspects that were reviewed, highlighting potential deficiencies over a range of financial and economic conditions, and determining whether adjustments or other compensating controls are warranted. Effective validation reports include clear executive summaries, with a statement of model purpose and an accessible synopsis of model and validation results, including major limitations and key assumptions.

Summary of OCC Bulletin 2000-16 Risk Modeling: Model Validation

The guidance outlines key model validation principles and the OCC's expectations for a sound model validation process.

Key Excerpts

The internal logic of most models is usually very abstract and limiting, so it requires considerable judgment and expertise to apply model results outside of the narrow context under which they are derived.

The OCC has observed several instances in which decision makers either relied on erroneous price or exposure estimates, or on an overly broad interpretation of model results, with serious consequences for their bank's reputation and profitability.

Sound model building includes rigorous procedures for "model validation." Model validation not only increases the reliability of a model, but also promotes improvements and a clearer understanding of a model's strengths and weaknesses among management and user groups.

A model consists of three components: An information input component, a processing component and a reporting component. Since errors in any of these three components can cause the model's information to be meaningless or misleading, an effective model-validation process must address all three components.

In practice, model validation requires not only technical expertise but also considerable subjective business judgment. It is important for decision makers to recognize that this subjectivity elevates the need for sound and comprehensive validation processes.

When validating a model, three procedures are applicable:

- 1) Independent review of the logical and conceptual soundness
- 2) Comparison against other models
- 3) Comparison of model predictions against subsequent real-world events

One or more of these three procedures should be applied to the model's three components: 1) information input, 2) processing component, and 3) reporting component.

Elements of a Sound Validation Policy

Independent Review – Model review should be as independent as possible from the personnel who construct the model.

Defined Responsibility – Model validation should be as formalized and defined as model construction. Internal audit should verify that before a model is put into production, an independent model validation should occur. This will include documented testing procedures and reasons for concluding that model is valid for intended uses.

Model Documentation – A model inventory should be maintained at the corporate level. Documentation should be sufficient to facilitate independent review and training of new staff as well as to demonstrate clear thinking by the model developer. At a minimum, model documentation should provide summary overviews of the general procedures used and the reasons for choosing those procedures, describe model applications and limitations, identify key personnel and milestone dates in model construction, and describe validation procedures and results.

Ongoing Validation – It is understood that models will be modified and updated as processes and business functions are better understood. Changes to key assumptions should be documented and submitted for independent review. Change-control procedures should also be implemented to prevent unauthorized and unapproved changes to key assumptions.

Audit Oversight – While model validation is likely to be outside the scope of the internal audit function, internal audit is responsible for ensuring that models are validated according to policy requirements.

Validation of Model Inputs Component

Data - Ensuring the quality of these data inputs is the first step in establishing a quality modeling process. Policies should ensure that internally sourced data should agree with the bank's general ledger data, actual contract terms, and data reported to regulatory authorities. Automated filters and product experts should be utilized to validate data inputs. Where data quality is suspect or cannot be fully validated, policies should specify that audit, risk management, and modeling personnel are independently responsible for informing senior management of the data problems.

Assumptions – Modelers should provide a clear rationale for key assumptions such as mortgage prepayment speeds, core deposit decay functions, interest rate volatilities, etc. Some assumptions will be sourced from internal models of bank customer behavior. These models will also need to be independently validated for

accuracy. Assumptions for product and portfolio behaviors should be frequently compared to actual behaviors. For key model assumptions, it is good practice to provide comparisons of projected versus actual behavior to senior management.

Validation of Model Processing Component

Code and Mathematics - The validation policies for the processing component of both internally developed and vendor models should ensure that the mathematics and computer code are error free. If vendor models are utilized, a bank may not safely assume that the models work because they are market-tested. Where available, source code should be reviewed for accuracy. Where this is not possible, to the extent feasible, independent models should be constructed to validate computations.

Theory – One of the largest sources of model error arises in the use of theoretical tools, most often statistical methods, by untrained modelers. An independent review of the theory that the bank uses in constructing its models is an essential element of validation.

Validation of Model Reports Component

Reports provided to senior management and key decision makers should be reviewed as part of the model validation process. Model results should be compared against those of comparable models, market prices, or other available benchmarks. Model estimates should be “back-tested;” that is, they should be frequently compared to actual outcomes and financial results.

Reporting context should be considered and addressed. Reports for senior management and decision makers should contain an executive summary that clearly states the purpose of the reports, limitations for use as well as key assumptions used in producing model results. A model review should ensure that results are clearly and effectively communicated to key decision makers. Best practices also include the use of sensitivity analysis to key model assumptions as well as “what-if” scenarios and stress tests.

Summary of Supervisory Expectations

“Using unvalidated models to manage risks to the bank is potentially an unsafe and unsound practice. Even where the risk is not particularly material, the reliance on unvalidated models can be a poor business practice.”

The OCC expects that a bank’s policies ensure that the following goals are met:

- 1) Decision-makers understand the meaning and limitation of models and associated results. Model outputs should be transformed, where necessary, into useful decision-making information without obfuscating the model’s limitations.
- 2) Results are tested against actual outcomes.
- 3) The bank should audit the model inputs. Input errors should be communicated and addressed in a timely fashion.
- 4) Seniority of management overseeing modeling process should be commensurate with the materiality of the risk.
- 5) Model validation should be independent from model construction.
- 6) Responsibility for key elements of model validation should be clearly defined.
- 7) Modeling software should be covered by change-control procedures.

Summary of "Model Governance," FDIC¹⁰

While financial modeling has become increasingly important to the banking industry, it has introduced a new source of risk, model risk. 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
- Promoting better management understanding of the limitations and potential weaknesses of a model.

The article discusses:

- The use of models in banking
- A conceptual framework for model governance
- 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

Financial models serve many purposes for financial institutions, such as informing decision making, measuring risk, and estimating asset values. Examples include:

- Credit scoring models *inform decision making*, providing predictive information on the potential for default or delinquency used in the loan approval process and risk-based 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.

Models are used to determine 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

¹⁰ Article in Supervisory Insights, Winter 2005, Vol. 2, Issue 2.

regulatory capital held for market risk exposure.¹¹ At institutions adopting the Basel II capital standards, 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. 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. While such spreadsheets might not be thought of as "models," their output directly contributes to preparation of the institution's reported financial statements, and adequate controls are necessary, given the seriousness of any potential errors.

Conceptual Framework for Model Governance

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. While procedures will vary, core model governance principles will apply at all institutions:

- The board establishes policies providing oversight throughout the organization commensurate with overall reliance on models.
- Senior management or business line management 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

Examiners are not expected to 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. In addition, they will consider findings of the bank's internal audit staff. The evaluation of model use and governance often becomes critical to the regulatory assessment of risk in the reviewed activities. Regulatory review typically focuses on the core components of the bank's governance practices by evaluating:

¹¹ Institutions with \$1 billion or more in trading assets are subject to the 1996 Market Risk Amendment to risk-based capital regulations.

- 1) Model oversight
- 2) Model control practices
- 3) Model validation.

Model Oversight

When evaluating board and senior management oversight, examiners typically review:

- model governance policies to determine adequacy and compliance with established policies
- the bank's model inventory for accuracy and completeness.

Model policies:

- Define a model, identifying what components of management information systems are considered subject to model governance procedures
- Establish standards for controls and validation
- Normally require verification of control procedures and independent validation of model effectiveness before a model is implemented as well as exceptions to the use of unvalidated models
- 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: A model 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 discussions of model theory, limitations and potential weaknesses, and operating procedures
- Review data reconciliation procedures and business line analysis of model results
- 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 should provide a thorough understanding of how the model works and allow a new user to assume responsibility for the model's use. 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

Data integrity:

- Business line management is responsible for the regular reconciliation of source system information with model data to ensure accuracy and completeness.
- 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.

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.

Change control is used to ensure all changes are justified, properly approved, documented, and verified¹² for accuracy. Events covered by such procedures include:

¹² 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.

- the addition of new data inputs
- changes in the method of data extraction from source systems
- modifications to formulas or assumptions
- changes in the use of the model output

Model Validation

Validation is not 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 should be completed before a model is put into use. 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 will test the effectiveness of the bank's validation function by selectively reviewing various aspects of validation work performed on individual models. When reviewing validations, 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
- Assess the qualifications of staff or vendors performing the validation.

Components of Validation include:

- Developmental evidence
- Process verification
- Outcome Analysis.

Developmental evidence: This component relates to the conceptual approach and quantification techniques of the model itself. A 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 covers:

- Data inputs
- The workings of the model itself
- 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. Verification 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 such as:

- Qualitative reasonableness checks that consider whether the model is generally producing expected results
- Back-testing a direct comparison of predicted results to observed actual results
- Benchmarking of model output to with predicted results from other models or sources.

Additional Considerations

A complete review of model validation will incorporate an analysis of the expertise and independence of model staff. 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, an external vendor or combinations thereof. 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 validators 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.

Summary of FFIEC Guidelines on Interest Rate Risk Management

The Federal Financial Institutions Examination Council (FFIEC) released an advisory on January 7th, 2010 reminding institutions of supervisory expectations for sound practices to manage interest rate risk (IRR). This advisory, adopted by each of the financial regulators, reiterates the importance of:

- Effective corporate governance;
- Policies and procedures;
- Risk measuring and monitoring systems;
- Stress testing, and
- Internal controls related to the IRR exposures of depository institutions.

It also clarifies elements of existing guidance and describes some IRR management techniques used by effective risk managers.

The following analysis describes the most important concerns outlined in the Statement. In addition, key differences between this statement and previous regulatory statements (primarily the 1996 Joint Interagency Policy on Interest Rate Risk Management as well as OCC 200-16 on Model Validation) are noted.

- The Federal regulatory agencies are aware that many institutions are taking advantage of the low level of short term rates and the steepness of the yield curve by borrowing short and lending long. There is a concern that an increase in rates, which many expect to occur in mid-2010, could severely compress margins for banks engaged in this strategy. Senior management needs to be keenly aware of any strategies that are driven by the current shape of the yield curve.
- The Board of Directors is ultimately responsible for the institution's measurement, monitoring, and management of IRR and should be aware of their responsibility to understand exposures as well as approve strategies to mitigate IRR.
- There is a heightened degree of concern that measures of IRR be reported correctly to ALCO and the Board of Directors to support their understanding of exposures to IRR.
- The relationship between IRR and other risks (especially liquidity risk) should be clearly measured and understood at the senior management and Board of Directors level.
- Institutions should have explicit measures of and limits on basis, yield curve, and options risk if these exposures are material.

- Institutions should evaluate exposure to both earnings and the balance sheet/capital. The explicit reference to understanding balance sheet risk in addition to equity/capital-at-risk is especially notable.
- Earnings at risk should be projected over at least two years (as opposed to one year in previous statements).
- Products with embedded options (primarily mortgage-related assets) should have their risks evaluated over 5 – 7 years.
- Earnings at risk simulations should take into account both static and dynamic balance sheet assumptions, especially regarding growth in balances.
- Stress testing should look at scenarios of ± 200 , ± 300 , and ± 400 basis point shifts (as opposed to ± 200 basis point shifts in previous statements).
- In low rate environments, scenarios involving significant declines in market rates can be de-emphasized. The potential for negative nominal or real interest rates should not be ignored, however.
- Sensitivity analysis (prepayments and core deposit behaviors as opposed to the interest rate scenarios listed above) should be evaluated to help determine which assumptions have the most influence on model output.
- Interest rate exposures need to be incorporated and evaluated as part of an institution's enterprise-wide risk identification process (ERM).
- Institutions must document, monitor, and regularly update key assumptions used in IRR management for senior management's approval.
- Behavioral models – for prepayments, core deposit decay, and key rate drivers – are critical for successful IRR management.
- Model validation is important – but the underlying code and algorithms for vendor models do not have to be reviewed if the vendors can provide documentation indicating that third parties have recently conducted these reviews.

Angel Oak Advisory

Angel Oak Advisory risk management consultants collaborate with bank management bringing thoughtful solutions based on practical, real-world experience underscored by extensive theoretical knowledge.

Angel Oak works within each client's parameters as well as its culture to develop and implement risk management solutions. Every assignment receives intense attention through each stage of the engagement. In addition, our highly efficient processes and team-oriented approach are designed to maximize results.

Angel Oak's senior-level team members forged their wealth of knowledge not only in prosperous times but also during periods of extreme financial stress. Their real-world experience has fostered an exceptional perspective that truly differentiates Angel Oak from other firms serving the financial community.

We look forward to working with you.

David J. Green Ph.D., CFA

David Green has more than 15 years of experience in risk management at various financial institutions and with regulatory authorities. Prior to joining Angel Oak, he served as the Treasurer of BankUnited FSB, where he was responsible for investment portfolio management, wholesale funding, derivative strategies, secondary marketing, funds transfer pricing, and ALM.

David was previously the ALM manager at SunTrust Bank, where he managed the interest rate risk modeling team. He is a former chairman of the Georgia Bankers Association's ALM Committee. He was also a capital markets specialist in Supervision and Regulation at the Federal Reserve Bank of Atlanta, where he was responsible for evaluating the risk management practices of banks and bank holding companies. He also developed and delivered risk training material for examination staff.

David earned a Ph.D. in Economics from Georgia State University and a B.S. in Mathematics from the Georgia Institute of Technology. He is also a CFA charter holder.