

OFHEO

Office of Examination and Oversight

Examination Guidance

Issuance Date: February 12, 2001

Doc. #: EG-2001-01

Subject: Examining for "Model Exposure"

To: All OFHEO Examining Personnel

The Office of Examination and Oversight (OEO) is committed to an effective, efficient, and transparent Examination Program. A critical component of OFHEO's risk-based examination and oversight process includes the ongoing review and assessment of its program. We have concluded the Examination Program would benefit from greater transparency in our approach for examining for "Model Exposure".

When assessing the quality of risk management, OFHEO's examiners routinely evaluate the quality of the tools and processes used by the Enterprises, as well as the quality of the personnel who use the tools, execute the processes and implement Enterprise practices. This Examiner Guidance provides general instruction for OFHEO's examiners who evaluate the Enterprises' use of automated models and other sophisticated quantitative (mathematical) techniques in their selection and management of risk. In addition, this Guidance addresses issues related to the Enterprises' "model exposure", including the sources and consequences of model exposure, and the control of model exposure through validation of quantitative methods and methodologies. By following the examination approach outlined in this Guidance, OFHEO's examiners will be positioned to opine on both the quality of the Enterprises' computer models and quantitative techniques, as well as the control environment that surrounds these tools.

The examination activities described in this Guidance are consistent with and complement OFHEO's Examination Program that is described in Chapter 2 of the *Examination Handbook*. This Guidance provides expanded direction to examiners for their use in assessing the risk framework associated with each of the examination program areas.

Attachment

G. Scott Calhoun
Chief Examiner

Examining for “Model Exposure”

Purpose

Routinely, examiners evaluate the quality of the tools used by management in tandem with an evaluation of the quality of personnel and processes when evaluating the overall quality of risk management. This issuance provides general guidance for OFHEO’s examiners who evaluate the Enterprises’ computer models and other quantitative techniques to select and manage risks. In addition, this document addresses issues related to the Enterprises’ “model exposure”, including the sources and consequences of model exposure, and controlling model exposure through validation of quantitative methods. Through the approach outlined, OFHEO’s examiners will be positioned to opine on the quality of the Enterprises’ models, along with the control environment that surrounds these tools.

Background

The Enterprises, like many other financial institutions, use a variety of computer models and quantitative techniques to deliver and price products and services, as well as manage their portfolios of risk. Computer models are vital tools needed by the Enterprises to process the vast amounts of information at their disposal. These models can provide analytically rigorous measurements of risks and are intended to aid management in objectively measuring risk, controlling risk, pricing financial instruments, and improving business decisions. Models are used for a wide variety of activities, including asset/liability management, assessing borrower creditworthiness, measuring performance, evaluating and selecting risks and transactions, forecasting future earnings, estimating values of financial instruments, managing capital allocations, assessing hedging strategies, and evaluating business opportunities.

While computer models and mathematical techniques are designed to be effective management tools, undue reliance on them for business decision-making and risk management introduces “model exposure”. While models can provide for methodical and rigorous analyses, a flaw or material error can result in unexpected, unintended, or misstated risk. In recent years, high-profile cases have been reported where faulty modeling has had adverse financial impacts on several financial firms. These examples serve to highlight the need for rigorous controls and management oversight when models are used to provide information for management’s decision-making and risk-taking.

In response to these cases, regulators now stress the importance of model reliability – not just when the models are introduced, but as long as the models are used. Financial regulators highlight the need to periodically review and validate the data, methodologies, and assumptions used in quantitative models. Financial regulators are also concerned with over-reliance on any single risk measure or quantitative tool. The regulators appropriately stress that while the quantitative side of risk management is improving

rapidly, effective risk management involves a blend of qualitative and quantitative information. In other words, models and quantitative techniques should complement the “human factor”, which incorporates experience and an intuitive understanding of markets, human behavior, and the environment.

Sources & Consequences of Model Exposure

Model exposure is the risk that poor business decisions will result from a model that is: flawed in its logical operations; incorrectly applied; or inappropriately applied. For purposes of this Guidance, a model is considered to have three components:

- A set of information or data inputs (e.g. financial positions, customer information, market conditions, historic information, etc.);
- Computer programs that employ mathematical and logical operations to process information to produce quantitative estimates; and
- A reporting system that allows management to incorporate these quantitative estimates into the decision-making process.

Material errors or flaws can inadvertently arise in any of these three components. For example:

- Input information can be missing or in error;
- The computer program or the mathematical logic can be flawed;
- Even if the information inputs and computer programming are reliable, there may be mistakes in the reports (output); or decision-makers can misinterpret the model’s output or conclusions.

The ways in which model errors can lead to poor decision-making varies. However, some common examples of model exposure are:

- *Misestimate of Risk:* A model can either overstate or understate the level and nature of risk associated with particular transactions, portfolio of financial instruments, or line of business. If a model overstates risk, the decision-maker may forego a profitable business opportunity. If a model understates risk, a decision-maker may make an unprofitable transaction or unknowingly expose the company to inappropriate risks.
- *Poor Risk Selection:* Faulty models can lead to poor portfolio choices and risk selection. For example, inaccurate data or programming errors can cause a credit-scoring model to incorrectly rank potential borrower’s creditworthiness. The cumulative effect of such an error may have adverse consequences on the portfolio’s profitability and the goal of fulfilling legitimate credit needs.
- *Misallocation of Capital:* Since capital allocation depends on complex risk and return measures, model errors can lead to an inappropriate allocation of the capital resources across lines of business and portfolios of risk.

- *Inappropriate Drivers for Organizational Behaviors:* The drivers of organizational behavior may be inappropriately influenced by errors in measurement and reporting. If there is flawed information, an organization may find its individual decisions and transactions to be in conflict with its defined goals and objectives.

Controlling Model Exposure

Controlling model exposure, commonly referred to as “model validation,” requires minimizing errors in each of the three model components. Model validation is necessary to ensure the accuracy and reliability of model inputs, computational processes, and the model estimates generated.

Implementing a model can be a substantial, systems-intensive procedure. Beyond the information technology challenges, we expect each GSE to have a company-wide standard that protects the Enterprises from relying on flawed models. At a minimum, the standard should define the process or principles employed across the organization to ensure that models are “valid” and surrounded by the appropriate control environment. Standards for the control environment should outline:

- the controls assuring the quality of data inputs;
- the controls assuring the logical operations and mathematical computations maintained in the code; and
- the controls assuring that risk measurement reporting is accurate and the related systems are sound.

Accordingly, management should ensure the following:

- An independent, formal vetting and validation process is present to approve models (including modifications), the quality of assumptions and the integrity of the data sources. Independence is defined as the meaningful involvement of qualified individuals who are not directly involved in the discrete risk-taking decisions for which the model is being used, and whose compensation is not directly related to what the particular model is estimating.
- The model’s methodologies (data sources, formulas, parameter selection, etc.) are protected and documented. The documentation should include a description of the transactions and circumstances in which the model may be appropriately used
- An independent review is periodically conducted to verify the completeness of data capture, correctness of model inputs, and the accuracy of results from the mathematical and logical operations. The periodic reviews need to be conducted by parties with the appropriate level of expertise to add credibility to the assessment.
- The GSEs should implement precautions to ensure that the loss of a few key personnel does not impair their ability to operate or maintain the reliability of the models and maintain the appropriate elements of independence.

Audit is expected, at a minimum, to play a baseline role in assuring models are reliable and operating within an appropriate control environment. In addition to testing for internal controls and checking for independence, audit should verify that the model inputs are consistent with general ledger and counterparty information, and that reasonable procedures and controls are in place to derive third party data used to run models. Audit should perform sufficient verification work to attest that computer programs are coded correctly and that the underlying mathematical and logical operations are consistent with the documented standards and methodologies.

When practicable, it is desirable to supplement internal processes and audit reviews with independent peer reviews by modeling professionals. Independent peer reviews are particularly useful for addressing the validity of the model's mathematical and logical operations, and the clarity of reports used to communicate model estimates to management.

OFHEO's Examination Approach

Sound risk management is vital to the prudent operation of the Enterprises' businesses, and is grounded in good risk measurement. Examiners should remember, however, that there are no sophisticated analytics that can replace experience and sound professional judgement when selecting and managing risks. Therefore, the Enterprises' computer models and quantitative techniques should be viewed as tools that support, but do not supplant, management's decisions and judgements when selecting and managing risks. Excessive reliance upon these tools that is not supported by human judgement or an appropriate control framework is considered imprudent.

In evaluating safety and soundness exposure to models, OFHEO has structured its evaluations to complement the routine examination work conducted in accordance with the program detailed in this *Examination Handbook*. When reviewing computer models and quantitative techniques, examiners are directed to evaluate the quality of the Enterprise's control environment that surrounds the models and the quality of model validation in each of the three components discussed in this *Examination Guidance* consistent with the purpose and use of the model. Examiners must consider if models reliably and adequately support management's identification, monitoring, and evaluation of risk. When conducting a review of models, examiners will consider the questions in this section of the guidance, as appropriate.

General Questions:

- Does management maintain an inventory of the substantive models used in financial and risk-taking decisions?
- Does the model identify and measure the relevant risks? What risks were identified?

- Does the validation process reconcile the stated or desired level of risk with the actual risk resulting? What are the results of this reconciliation?
- Are the models and data inputs appropriately selected?

Questions Covering the Data Input Component:

- Is there a rigorous process for ensuring and validating quality data inputs? What were the results of this validation process?
- How is this process tested?
- With what frequency will this process be tested?
- How are the approved processes for data input protected?
- What is the quality control process? What were the results from the quality control process?

Questions Concerning the Mathematical and Logical Operations Component:

- What are the mathematical and logical operations for this model operation?
- How were the mathematical and logical operations of the model validated? What were the results of this validation?
- How, by whom, and under what circumstances can the mathematical and logical operations be tweaked or changed? When these mathematical and logical operations are tweaked or changed, what is the requirement for re-testing or re-validation?
- Is there a defined frequency for when the mathematical and logical operations of the model are routinely rechecked?
- Do the mathematical and logical operations of the model seem reasonable?
 - Are the mathematical and logical operations likely to generate conservative results?
 - Are the mathematical and logical operations likely to generate aggressive results?
 - Are the mathematical and logical operations adequately documented?
- What are the major assumptions used in the model? Are they adequately documented and appropriately supported?

- How do the mathematical and logical operations of the model, and the assumptions driving the model compare with generally accepted methodologies and/or market conventions?
 - If not, can the Enterprise provide sound support and analysis for these differences?
 - If not, what is the nature and magnitude of the variance in the output as a result of these differences?
- Where there are differences, do these differences affect the reliability of the results as they are being used for decision-making? If yes, describe the nature of the differences.

Questions Covering the Reporting Component:

- How are the model outputs incorporated into management and decision-making tools? How does management assure itself that the metrics being incorporated result in reliable information for decision-making?
- Are the outputs being appropriately characterized in management reports?
- Does the presentation of the outputs create any bias in the decision-making process?
- Does incorporating the model outputs enhance management's ability to prudently manage risk and make business decisions?
- When changes in data inputs or mathematical and logical operations alter the outputs, how are decision-makers informed and educated about the change?
- What are the quality control processes, and how are outputs reviewed to detect any potential problems resulting from bad data and faulty assumptions?

Summary Questions:

- Is this model a reliable tool for use in management's decisions to select and price risk?
- Is this model a reliable tool for use in monitoring and managing risk?

Summary

The purpose of this Examination Guidance is to instruct OFHEO's examiners on the process for use in evaluating model exposure. The process details an assessment framework that ensures the Enterprise has an appropriate control environment and

conducts sufficient testing and validation to rely upon the results of its automated tools and quantitative techniques. Examiners will couple these assessments with the assessments generated through the other examination areas to determine the alignment of these risk management tools with the human judgements and business practices of the Enterprise.