Technology Is Great, But Remember to Validate

By Scott R. Fryzel, Partner, Chapman and Cutler LLP

Technology continues to take an expanded role in banking and the way consumers and businesses manage their money and lives. Banks and other financial institutions increasingly rely on various types of models to make decisions and manage the risk in providing consumer and commercial services. These models include credit scoring, interest rate risk analysis, models for decisions of consumer and commercial credit, and whether to permit or decline a transaction (including risks for OFAC violations and money laundering). Many of these models are provided by third-party service providers or vendors.

In 2011, the Office of the Comptroller of the Currency and the Board of Governors of the Federal Reserve issued joint Supervisory Guidance on Model Risk Management[1] (Guidance), recognizing that banks rely heavily on quantitative analysis and models in most aspects of decision making. The guidance observed that banks use models for a broad range of activities, including underwriting credits; valuing exposures and positions; measuring risk; managing and safeguarding client assets; determining capital and reserve adequacy; and many other activities, such as enterprise risk management. The guidance warns of the possible adverse consequences (including financial loss) of decisions based on models that are incorrect or misused, and advises that these risks should be addressed by active management of model risk.

Guidance Summary Re: Model Validation

The guidance includes a specific requirement for financial institutions to validate the models it uses as part of its business, whether obtained from third-party vendors or developed and implemented in-house. We often see this requirement overlooked by bank clients as part of their vendor management program. After the often very intensive and time-consuming work that goes into the assessment and implementation of a model for use by a bank, the ongoing monitoring and validation of how that model is functioning is just as important and must be documented. This includes maintaining an inventory of the models used by the bank; listing the individual or group responsible for the model; documenting the products and purpose for which the model is designed; the actual or expected usage of the model; any restrictions on usage; and the dates of completed and planned validation activities.[2]

As part of its vendor risk-management program, banks are required to validate the models they use, or require the third-party vendor to validate its model, on an annual basis or more frequently if warranted. Validation of models is required to verify that they are performing as expected. The validation can affirm previous validation work, suggest updates to previous validation activities, or call for additional validation activities or revisions to the model. Where a third-party vendor's model is used, the requirement to validate or provide an independent validation report should be incorporated in the vendor's contract with the bank. [3]

1 OCC Bulletin 2011-12, Supervisory Guidance on Model Risk Management (April 4, 2011); FRB Supervisory Letter SR 11 7, Supervisory Guidance on Model Risk Management (April 4, 2011).
2 Id. at 20. 3 Id. at 15 16.

The guidance lists three key elements of a comprehensive validation framework:

1. Evaluation of conceptual soundness. This element involves assessing the quality of the model design and construction; reviewing documentation and empirical evidence supporting the methods used; and the variables selected for the model. The developmental evidence should be reviewed before a model goes into use and as part of ongoing validation whenever changes are made to the model.
2. Ongoing monitoring. Ongoing monitoring is used to confirm that the model is appropriately implemented and is being used and is performing as intended. Beginning when a model is first implemented into production systems for actual business use, ongoing monitoring is essential to validate that a model continues to perform as expected and to determine whether any changes are required.
3. Outcomes analysis. An outcomes analysis compares the model outputs to corresponding actual outcomes. This element helps evaluate model performance, assessing the reasons for any observed variation and effectively determining whether the results produced by the model make sense. 4

Special attention is given in the Guidance to the validation of vendor and other third-party products, including data, parameter values and complete models. These must be incorporated into the bank's model risk management framework following the same principles as in-house applications. This involves vendor selection, testing, defining a model's limitations and assumptions, and clearly outlining ongoing performance monitoring and outcomes analysis. Ongoing validation of the vendor application is necessary to make certain it functions as the bank intended, as well as to build as much in-house knowledge as possible in the event the vendor must be terminated. [5]

Management and the board of directors must establish and maintain adequate policies, procedures and a governance structure that are aligned with the extent and sophistication of model usage. This includes a strong risk management framework, ensuring compliance with policies and procedures, assigning competent staff, overseeing model development and implementation, evaluating model results, reviewing validation and internal audit findings, and taking prompt remedial action when necessary. A bank's internal audit function should also include an assessment of the overall effectiveness of its model risk management framework. [6]

4 Id. at 11 15. 5 Id. at 15. 6 Id. at 16 17.

"Whether a vendor is using a model as part of or for the full service provided, a bank should obtain a contractual commitment from the vendor to obtain an independent validation of the model on no less than an annual basis."

Recommendation

With the continued growth in outsourcing functions, we observe more models being implemented that are developed by third-party vendors and bank service providers, including core processors. Vendors that provide core processing to a bank may further subcontract the development, implementation and use of a model. Whether a vendor is using a model as part of or for the full service provided, a bank should obtain a contractual commitment from the vendor to obtain an independent validation of the model on no less than an annual basis. The validation should be scheduled, performed and recorded as part of the institution's vendor risk management program.

Banks should hold vendors accountable as true partners that will help the bank meet its regulatory requirements to validate models licensed or sold to the bank for the bank's business and service to its customers. IB

About the Author: Scott Fryzel is a partner in the Banking Department of Chapman and Cutler LLP, an IBA Associate Member, and represents U.S. and foreign financial institutions and finance companies on a broad scope of issues including bank mergers and acquisitions; regulatory activities and compliance; treasury management and payment processing; and outsourcing, white-label services and vendor management. He can be reached at 312-845-3784 or fryzel@chapman.com

Copyright 2013 Chapman and Cutler LLP