How Model Risk Management Can Play a Leading Role in Compliance

By Arthur R. Preiss, PhD., and Stephen E. Sudhoff, CFA

Models help us think about our world in a structured way. As credit products have become more complex and computing power has become cheaper and more accessible, analysis of more complex relationships has become easier. And, as our world has become more complex, our need for models has grown to help us think about various issues, and devise solutions to these issues. Model usage in compliance has also grown because models are a cost-effective way of dealing with the regulatory burden.

Many Types of Models Are Used in Bank Compliance Today

The models discussed in this article have compliance risk implications, and their governance falls under the auspices of risk management and/or the compliance function. For example, the compliance officer may be the assigned owner of a bank's fair lending model used to identify exposures due to credit underwriting and pricing decisions, a CRA data assessment system used to evaluate lending patterns, or models used to identify BSA/AML suspicious activity. Credit scoring or complaint analysis systems are other models that may be owned by other functional areas but warrant compliance risk management oversight. And, an example of models helping compliance officers deal with the growing regulatory burden is the coming analysis of the expanded HMDA data. These models may be developed internally or purchased from an external vendor depending on the preference of the institution.

Trends in Model Usage

In the past 25 years, we have witnessed an analytical explosion and a concomitant growth in modeling. In fair lending, the initial modeling effort involved differential treatment with respect to mortgage applicant race. Then, modeling expanded to include other prohibited basis groups such as gender, age, and marital status. Additional expansion included other credit products such as consumer secured and unsecured loans, HELOCs, direct and indirect autos,

small business, and credit cards. Furthermore, the analytics expanded from the credit and pricing decisions into other types of risk such as redlining. We now witness expansion beyond banks to mortgage companies and the like. Moreover, the recent amendments to HMDA that expanded the scope of data fields suggest a heightened analytical capacity for models using such data.

Outside of the fair lending explosion, BSA/AML monitoring has evolved from a largely manual process into a significant modeling effort that is well beyond point-and-click processes. The urgency of detecting terrorism financing post-9/11 certainly provided an impetus for the increased use of automated monitoring processes. Analysis now may involve machine learning or similar approaches, especially among service providers.

As a direct result of the development of the Consumer Financial Protection Bureau's (Bureau's) database, a new area of modeling is "complaints". At the start, modeling was applied on an ad hoc basis as a way to discover causes for observed results. More recently, the manual reviews of the past have been supplemented with basic analytics employing big data using machine learning or similar techniques. Big data can be used to supplement traditional statistical analysis to detect patterns not otherwise seen in the data. A particular area of interest is unstructured data (which many analysts have estimated comprises 80% of all data), such as raw text and voice recordings. Big data can be implemented using machine learning techniques which are available from several external vendors using your institution's data and perhaps external data. You may also have an enterprising individual in your institution that has the ability to create models internally. If so, the experienced compliance officer knows to connect as soon as possible with that individual to help shape the approach, understand the risks, and avoid the pitfalls. Let's consider a few.

Practical Considerations in Model Usage

While there are many benefits to using models, there are also some drawbacks or risks. The benefits are:

- **Ability to review all applications/transactions.** In fair lending analysis prior to using models, the applications to be reviewed were typically chosen by sampling. With regression modeling, all applications are reviewed as part of the analysis.

- **Quick identification of outliers.** As a result of the all-inclusive modeling effort, outlier applicants are quickly identified as part of the analysis output.

- **Easy identification of matching applications/transaction.** Not only are outliers identified, but given a set of matching criteria, matching applications for those outliers can be identified, when they exist. Thus, the output of matched pairs in the past are now matches to all similarly situated applicants, if they exist.

- **Increased precision in matching.** The operating protocol for models minimizes the judgment associated with some of the old matched pair analyses and permits matching across multiple criteria.

- **Efficiency and cost control.** Compliance officers (not to mention management) like this process since it is efficient (i.e. cost effective) compared to other, more manual analyses and it establishes a reproducible process that is not dependent on the availability of a staff person running the process.

- **Identification and explanation of factors highly correlated with the target of the analysis.** It can identify what key factors highly correlate with credit and pricing decisions, SAR decisions, money laundering and complaint remediation.

- **Early warning control.** Complaint analysis can give the institution an early warning on potentially unfair, deceptive, or abusive acts and practices.

Some of the more prevalent risks are:

- **Inaccurate/incomplete data.** Poor quality inputs can lead to inaccurate and possibly inappropriate outputs or conclusions.

- **Business Unit Input.** Creating models without the benefit of business unit input can lead to erroneous business models and their associated outputs. Erroneous outputs fall under two general types:

    (1) A transaction or practice is identified as posing heightened potential risk, when in fact it does not. An example is when numerous transactions related to a specific product, service or customer type are identified as potentially suspicious. With limited resources available to investigate each transaction, the bank may make a decision to avoid the origin of the risk (e.g. the product, service or customer), thus essentially engaging in "de-risking," A transaction or practice which poses heightened risk and is not flagged at all. One example is when an underlying pattern of lending discrimination is not identified because of the model formulation, data accuracy or missing data.

- **Understand your model so that it reflects how you do business.** Sometimes compliance officers and their staff rely on outside consultants to build their compliance models, then they neglect to understand the meaning of the inputs and outputs of the model in relation to their business unit.

- **Model results should be consistent with policies, procedures, and actual practices.** Another risk associated with models is not incorporating the actions indicated by the output of the models in the bank's policies and procedures. The model results may mean that policies and procedures need to be changed or remuneration may be required.

<u>Build vs. Buy Decision</u>

Whether you decide to build your own models or buy them from a vendor, there are some key variables to consider. If you are considering buying your models, think about the following:

- Costs: Costs will vary but include annual fees, costs for training, special systems add-ons or conversions if any as well as the expense for new hires if needed.

- Software: There may be a charge for software updates. In addition, there could be hourly charges to assist bank personnel in the installation of the updates.

- Usage: The model may require special expertise such as statistical knowledge and on-going training for experts. In addition, if the models are used infrequently there is often a learning curve the model builder will experience such as re-learning the software syntax for making changes to the model. Finally, some models may be made available to be shared by multiple banks, e.g., underwriting and pricing models. Using shared models often results in the individual bank-unique business models being overlooked in the generalized model, and as a result, possibly producing inaccurate and perhaps misleading results.

- Vendor: Vendor reputation and capacity to support the product is critical. For example, does the vendor have support resources, and are they readily available to support use of the model? What is the feedback from other institutions about the product and vendor support? Waiting one or two days for a call back from a vendor about your question is very disappointing. Does your staff understand the special methodologies such as the analysis process and proxies, as well as the meaning of the output?

- Information Security: Almost certainly personally-identifiable information and sensitive company information will be shared with the vendor as part of any model. The information must be adequately protected (and ultimately returned/destroyed) and the vendor should be restricted from using the information for any other purpose. The institution must also need to understand the use of other data that may be part of the model.

If, on the other hand, the choice is to build the models in-house, the following key considerations are relevant:

- Does the bank possess model building expertise and is bank staff sufficiently available to execute the build and roll out to bank in a reasonable period? Model building is part science and part art. The exact amount of time or resources that it takes to build a

model is often difficult to accurately estimate. The last thing you want to do is to short-change the time and effort involved in building a model.

- Are controls in place to ensure the integrity of the data supporting the model, e.g., availability and accuracy of data?
- Does the bank have the expertise to make the best decisions to ensure a successful model building effort, e.g., types of computers and appropriate software?
- Does the bank staff have relationships with regulators and other external model builders to assist them with the inevitable questions that arise in the model building exercise?

Model Validation

Supervisory Guidance: With the increasing use of models, banking agencies have issued guidance to outline expectations for sound risk management involving these systems. For example, in 2011 the Board of Governors of the Federal Reserve System (FRB) and Office of the Comptroller of the Currency (OCC) issued Supervisory Guidance on Model Risk Management (Joint Guidance).[1] More recently in 2016, the FDIC proposed supplemental Third-Party Lending guidance (FDIC Proposal) that incorporated Model Risk as a key supervisory risk category.[2]

The Joint Guidance encourages model validation to ensure the soundness of the system and describes it as "…the set of processes and activities intended to verify that models are performing as expected, in line with their design objectives and business uses." The Joint Guidance identifies potential limitations and assumptions to be considered and assesses their possible impact, e.g., "…if credit risk models do not incorporate underwriting changes in a timely manner, flawed and costly business decisions could be made before deterioration in model performance becomes apparent." It also advises that validations "be performed by staff with appropriate incentives, competence, and influence."

The FDIC Proposal underscores the importance of independent verification of third-party models both prior to and after implementation. It also suggests that third party lending models may be particularly subject to fair lending risk given the limited history of some models in the marketplace.

Validation Timing: There are three phases in model use in which model validation is important. First, model validation needs to occur before the model is put into use. This validation is typically performed when the model is being developed and involves the statistician, the business line, and the Compliance Department. The second phase is when a model is changed. This may reflect when new software is installed, or additionally when the underlying business changes significantly, such as when underwriting or pricing guidelines change, or when the institution either acquires or expands a line of business. The final validation phase is periodic. This may only occur every few years, and is usually done to accommodate more up-to-date data samples. It will, however, usually be evident from model performance when revalidation will be needed.

Key to success: A crucial part of the validation process is that the financial institution understands the model and its outputs. The institution must know whether the model specification correctly reflects the institution's business model, that is, at its most basic, whether the model is attempting to measure what the institution needs to have measured. The institution must likewise invest the time and personnel to understand the model outputs; what they mean and, importantly, what they don't mean.

Practical steps in model validation: The first step is ensuring data accuracy. What we hear (and see in enforcement actions) is that institutions run into problems when data is incomplete, particularly when data (such as account activity recorded in core systems) is not appropriately transferred to the model (either through outright exclusion or by incorrect mapping). The institution must establish rigorous and comprehensive testing procedures to assure that data is regularly (even continuously) validated. Key to this process is a solid set of exception reports

which contain simple metrics, such as whether the number of transactions contained in the core system equals the number of transactions processed by the model. The institution must also have a process for reviewing these exception reports, and must empower staff to escalate exceptions.

Ideally, the responsibility for production of valid data should reside with the producer of the data. The role of Compliance is to ensure that there is a validation process (such as a risk control self-assessment process) in place with the data producer to ensure that there is a way of clearing exceptions.

Now let's turn to the validation of the model itself (assuming the incoming data is accurate). First, identify the variables (also called elements, factors or attributes) that are used in the model. This could be particularly difficult when engaging a vendor, since vendors may include variables not known to the institution. For a fair lending model, the variables might include underwriting/guidelines, or non-guideline variables, such as discounts. Then, run the model (press "GO"). Check the signs on parameters and the magnitudes associated with each parameter, and determine whether or not they make sense from a business perspective (for example, whether applicants with higher credit scores tend to receive preferred rates), and also from a compliance perspective (whether suspicious transactions are spread across different geographies, customers, etc.). Don't discount the value of the compliance officer's instincts or the effectiveness of this "smell test" step.

The next step (in both change validation and periodic revalidation) is to compare current period results with those from the previous validation. The institution should analyze whether certain factors have become materially either more or less important than in previous results. Of course the term "materially" needs to be defined for each model. The institution must investigate whether any changes in model parameters, variable signs, etc., are consistent with the expectations of the business line as well as that of Compliance. The institution should pay special attention to unusual results, such as variable signs for fair lending that appear to be incorrect, a sudden increase in suspicious activity from a specific geographic area, an increase in

complaints associated with a product which is being phased out, or significant changes in census tract income which could impact the CRA strategy.

The institution may need to re-estimate the model based upon these discussions, and then repeat the review process. The institution would ideally have standards in place for determining which variables to use as well as thresholds for determining that the model is still working properly. The institution should retain all of the documentation used in the review process.

Continuous Validation: Periodic validation protocols are essential, but ongoing and continuous validation outside of those protocols is extremely helpful to finding model errors. The financial institution should have a series of daily, weekly, and/or monthly "change reports" to highlight significant period-to-period differences in various metrics. Metrics could include the number of loans/transactions processed, number of suspicious transaction flagged by the system, numbers of complaints by type of complaint, etc. Significant changes in these metrics–even seemingly innocuous metrics–could be a "canary in the coal mine" serving to warn the institution of larger problems.

Periodic validation should also occur as model users notice differences in model results over time. As users gain experience and intuition they may notice when model results are different from what they expect. Users (especially junior staff) should be encouraged to investigate anomalous results and also escalate when they have persistent questions or concerns. An institution's policies and procedures should likewise give staff broad authorization to investigate anomalies based upon their own initiative. (This applies to senior staff as well–imagine how the 2017 Oscars would have been different had Warren Beatty simply said "I need some help. What is written on this card does not make sense to me.")

Validation of Proprietary Models: There is a category of model usage which can present significant issues for a model validator, that is, when a vendor model is used which has a significant proprietary component, such as a proprietary algorithm. Machine-learning techniques would typically fall into this category. From the vendor's perspective, the intellectual property (IP) embodied in proprietary techniques may be incredibly valuable, even perhaps the most valuable part of the vendor's franchise. As such, the vendor is unlikely to reveal the full nature of that IP to the customer. The model validator has a responsibility to ensure that the vendor's proprietary techniques work properly via independent review. One solution to this conflict is for the financial institution to require that the vendor engage an outside party to review any proprietary techniques. The vendor (and the financial institution) would need to assure that this outside party has sufficient expertise to perform the validation. The financial institution would be responsible for ensuring that the review met the validation standards of the model validator.

Inherent Risks to Model Usage

Models help us understand our new world better and are a cost effective way to manage some elements of compliance risk. However, there are inherent risks, and the Compliance Department has a key role in assuring that models are properly used within the institution. The Compliance Department must ensure:

- Models have complete and accurate data, including business unit input;
- Models reflect how your institution does business; you need to go beyond vendor default settings!
- Build vs. Buy is discussed, and understand the challenges of each;
- Models are validated before they are in use, when they are changed, and periodically thereafter;

- Their institution has standards for determining which variables to use, as well as the thresholds indicating when a model might not be working properly;
- A solid set of exception reports; and
- Staff is encouraged to escalate potential issues. Make sure that they are paying attention to results and are not off in La La Land.

Conclusion

While compliance risks are propelled by the same components that drive other banking risks, compliance risks are higher because of the possibility of unfavorable outcomes, such as regulatory actions. However, as models have improved, compliance personnel are able to use them to target necessary changes, and as a result, increase their efficiency and oversight capabilities. Institutions that take active ownership of these new modeling processes will not only be able to manage risk more effectively, but they will be able to reduce costs, increase service and have an overall competitive advantage.

ABOUT THE AUTHORS

Arthur R. (Rick) Preiss, PhD., President and Founder of Preiss&Associates, LLC., (www.preissco.com), works with all sizes of financial institutions to perform custom fair lending risk assessments, mentor in-house fair lending modeling processes, and collaborate to maximize software value. Located in Lake Forest, Illinois, Preiss&Associates has been a full-service compliance consulting firm since 1992, serving clients nationwide. Their unrivaled fair lending experience is utilized by financial institutions and law firms defending financial institutions, to perform a wide variety of of statistical fair lending analyses. Risk areas covered include underwriting and pricing and redlining for credit products.

Rick is a graduate of Emory University and received an MBA and PhD from Indiana University. He can be reached at rpreiss@preissco.com.

Stephen E. Sudhoff, CFA, is president of Jefferson Cook Associates, Ltd., a consulting firm focused on Fair Lending, Model Validation, BSA/AML, and CRA. His has thirty years of experience in the Chicago financial community, including extensive market and credit risk management leadership in large international banking and brokerage firms. He has both built and reviewed dozens upon dozens of models during his career. Steve holds an MBA from the University of Chicago and can be reached at Stephen.Sudhoff@jeffcookltd.com.

ENDNOTES:

[1] Board of Governors of the Federal Reserve System, Office of the Comptroller of the Currency, SR 11-7 Attachment SUPERVISORY GUIDANCE ON MODEL RISK MANAGEMENT, April 4, 2011, https://www.federalreserve.gov/bankinforeg/srletters/sr1107a1.pdf (retrieved February 2017)

[2] Proposed FDIC Guidance on Third-Party Lending (FIL-50-2016) https://www.fdic.gov/news/news/financial/2016/fil16050.html