A Closer Look

The Dodd-Frank Wall Street Reform and Consumer Protection Act

To view our other A Closer Look pieces on Dodd-Frank, please visit www.pwcregulatory.com

Part of an ongoing series

The evolution of model risk management

May 2013

Introduction

More than ten years since the Office of the Comptroller of the Currency ("OCC") issued its seminal OCC 2000-16 Risk Bulletin on Model Validation, a revised and significantly expanded set of supervisory guidance was co-issued by the OCC and the Federal Reserve (the "Agencies") in April 2011. While the exact reasons for this revised guidance are not publicly known, it is likely that the Agencies were reacting to observed systemic weaknesses in bank Model Risk Management programs under the prior guidance – including, based on our own observations during this time period, the following:

- The treatment of model validation as a compliance activity, as opposed to a risk management activity.
- Insufficient independence of validation testing and, accordingly, a lack of effective challenge.
- Outsourcing of model validation testing to third parties without appropriate involvement and oversight by bank risk management personnel.
- Insufficient and inconsistent scope of validation testing, and a focus of validation activities on "models" – instead of model uses.
- A focus on models being "valid" or "not valid" – rather than on identifying, and managing the risk of, model weaknesses and limitations – and the understanding of such by model users.
- Undetected deterioration in model performance over time due to lack of rigorous monitoring processes following initial model deployment and validation.
- Significant stress on the independent model validation function.

pwc

It is clear that the new guidance was designed to address these weaknesses through an expansion of detailed and, in some cases, prescriptive guidance on a bank's model risk management program. In particular, to dispel any notion that the Agencies are looking for a compliance-type function, and to highlight the degree of importance the Agencies place on model risk management, the guidance explicitly states that "Model risk should be managed like any other risk."

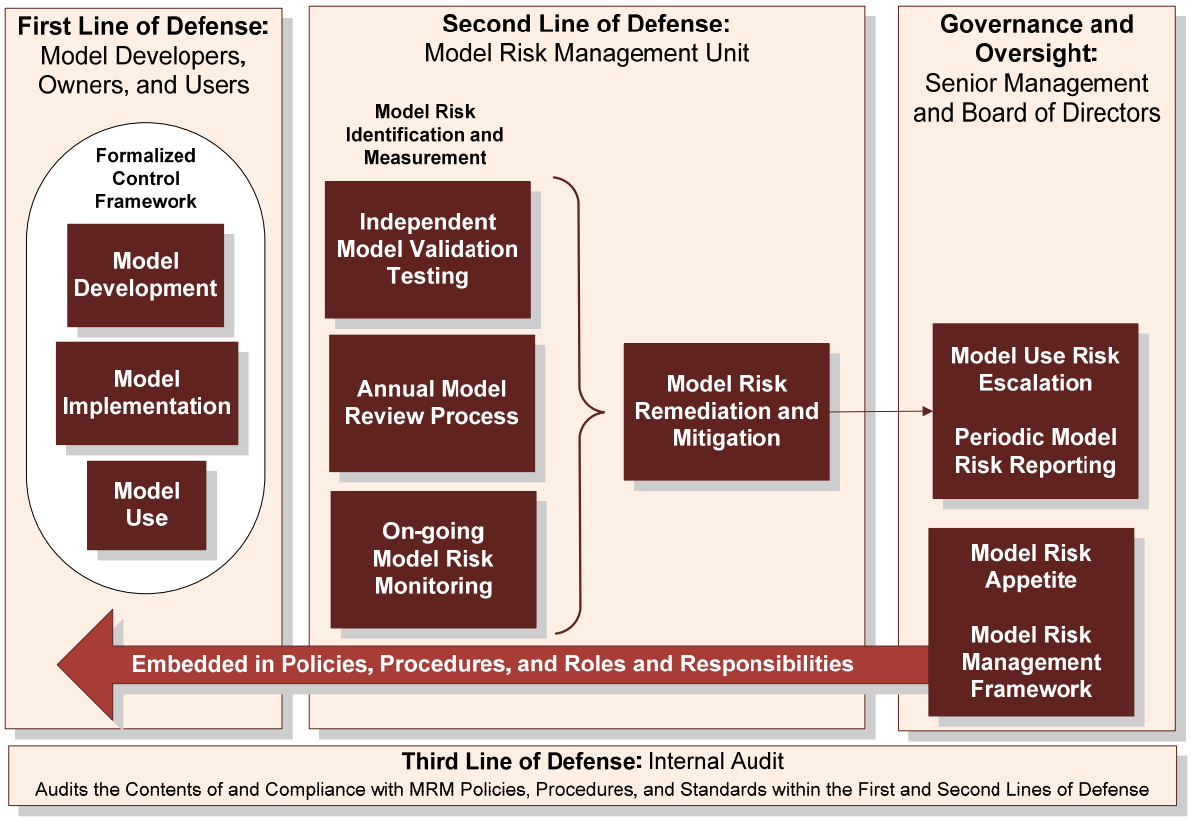
In the rest of the 21-pages of supervisory guidance, the Agencies lay out their expectations for governance and control activities for first, second, and third lines of defense – as well as specific guidance on more granular areas such as vendor models, model inventory, the use of external resources, and documentation. Taken as a whole, it is clear that the new guidance significantly raises the bar for banks by taking what used to be considered industry best practices and making them minimum regulatory expectations. Additionally, perhaps to drive more consistency in industry model validation testing practices, the Agencies have provided much more detailed, prescriptive guidance in all areas of model validation testing – including conceptual soundness, process verification, ongoing monitoring, and outcomes analysis.

While the new guidance is full of detailed information, we have observed a surprising degree of variability in banks' interpretations of this information both at a granular procedure level – as well as at a more macro programmatic and framework level. Accordingly, the goal of this article is to present our point of view on what this guidance means holistically for the bank, and to provide a high-level roadmap for evolving the model risk management function. From our perspective, this roadmap importantly includes:

- An expansion and formalization of first line control processes designed to mitigate model risk at its source.
- An evolution of the second line of defense program to include more dynamic, real-time identification and measurement of model risk.
- An evolution in program objectives away from whether models are "Acceptable" or "Valid", and toward a program focused on the long-term remediation, and short-term mitigation, of residual model risks to acceptable levels.
- An evolution of the bank model approval process to include roles and responsibilities for both the Model Risk Management Unit and key senior management use-specific governance/oversight committees. The former focuses on designing and monitoring technical model remediation plans with model owners, while the latter focuses on whether short-term risk mitigants proposed by model users reduce residual risks to levels consistent with the bank's risk appetite.

The model risk management framework

At its core, the new guidance envisions a more holistic enterprise-wide model risk management program with key roles and responsibilities assigned to all three lines of defense as illustrated below, and described more fully in the subsequent sections.



First line of defense: model developers and users

Model risk should primarily be mitigated or controlled at its source – that is: (1) by the personnel responsible for designing and building models for the bank (or, for vendor models, personnel responsible for selecting vendor models), and (2) by the personnel responsible for using models in such activities as business decision making, financial and regulatory reporting, risk management, or valuations. While the concept of well-controlled model development or use may seem obvious, the reality is that many banks have not had the type of formal, documented control processes around model development and implementation that one would expect.[1] Instead, model development groups typically follow certain practices that, while designed to improve model quality, have not typically risen to the level of formal control processes.

What this means is that banks will need to inject more formality into the model development and implementation control framework through the development of specific model risk control processes codified within such documents as "Model Development Guidelines/Standards" and "Model Pre-Implementation Testing Guidelines/Standards". These documents should specify the exact set of control activities expected for model developers and users in the following areas to control/mitigate model risks at their source:

- Model design and methodology.
- Internal and external data inputs and assumptions.

[1] The exception here is for models supporting financial reporting whose use has been subject to Sarbanes-Oxley control requirements since 2002. However, our experience is that a Bank's model risk management group (i.e., the second line of defense) is typically relied upon as the key control for model development and implementation. First line control processes are typically focused on the use of the model for specific financial statement line items.

- Model estimation and testing – including statistical validity, outcomes analysis, sensitivity analysis, and stress testing.
- Model deployment requirements – such as choice of model production platform, production data input requirements, choice of model software, model coding requirements, etc.[2]
- Selection and deployment of vendor models.
- Model pre-implementation testing.
- Model documentation requirements – both development and implementation.[3]
- Model output reporting.
- On-going model risk monitoring processes – including monitoring of: model performance, model operational process risks, model weaknesses and limitations, and compliance with any model risk mitigants required by the second line of defense.
- Identification and communication of key model risks, weaknesses, and limitations to model users – including risks associated with inherent model imprecision, key assumption sensitivities, and any risks identified through other first and second line control activities.
- Model approval process.
- Model change management process.

For many banks, this added formality will represent a significant evolution of first line processes; accordingly, it should be expected that such change will be both gradual and challenging – and likely require certain leadership efforts of the Model Risk Management Unit, as well as a supporting tone from senior management. Additionally, banks should plan and execute training activities at various first line levels to ensure clarity and consistency in the understanding of the new requirements and control processes. Finally, we expect that first line documentation requirements will require significant enhancements – particularly with respect to the documentation of control activity execution.

Of course, all of this increased formality comes at a cost, and banks will need to:

- Recognize that additional first line resources will likely be required to execute and document these control activities effectively.
- Build these control requirements (and corresponding impacts to project timelines) into model-build project plans.
- Develop a transition plan whereby legacy models are brought into compliance with these new control requirements.

Second line of defense: Model Risk Management Unit

From an overall strategic level, we view the roles of the second line of defense to be as follows:

- Monitor the effectiveness of the first line control framework through the performance of independent model risk identification and measurement activities.

---

[2] For further details on recommendations to mitigate model risks related to model production applications, see PwC, *Model Risk Mitigation and Cost Reduction Through Effective Design* (2009) available at www.pwc.com/modelrisk.

[3] For further details on recommendations to mitigate model risks through effective documentation, see PwC, *Model Risk Mitigation and Cost Reduction Through Effective Documentation* (2013) forthcoming at www.pwc.com/modelrisk.

- Ensure that appropriate short-term model risk mitigants and long-term remediation plans are deployed by model developers and users to reduce residual model risks to acceptable levels.
- Engage regularly with senior management and board governance/oversight groups with respect to the bank's model risk levels, proposed model-use mitigants designed to reduce model risk levels, and overall model risk management activities.

We discuss these more fully below.

Identification and measurement of model risk

Under the new supervisory guidance, gone are the days when the primary role of the Model Risk Management Unit ("MRMU") is to perform periodic model validation testing on a one-, two-, or three-year cycle – or when material changes occur to a model.[4] This legacy practice – while common across the industry and consistent with existing regulatory guidance – had the unintended effect of exposing the bank to emerging model risks between formal validation testing cycles. To close this gap, the MRMU is now expected to identify and measure model risk levels on a more dynamic, real-time basis using the following three processes:

- Periodic Model Validation Testing – conceptually, under the new supervisory guidance, the periodic model validation testing process is unchanged from prior practice; however, importantly, the Agencies have provided more prescriptive guidance on certain components of this testing – such as conceptual soundness, outcomes analysis, and validation testing of vendor models – that should create more consistency and promote greater rigor across the industry.
- Annual Review Process – in our view, unlike the rigor and scope of periodic model validation testing, this represents a more streamlined risk assessment process performed annually by the MRMU for all models in the bank inventory – including Low Risk models.
- On-going Model Risk Monitoring[5] – as with the Annual Review, the On-going Model Risk Monitoring process is another means by which the MRMU monitors, collects, and consolidates emerging model risk information; however, in this case, the model risk information may be generated from areas and activities outside of the MRMU.

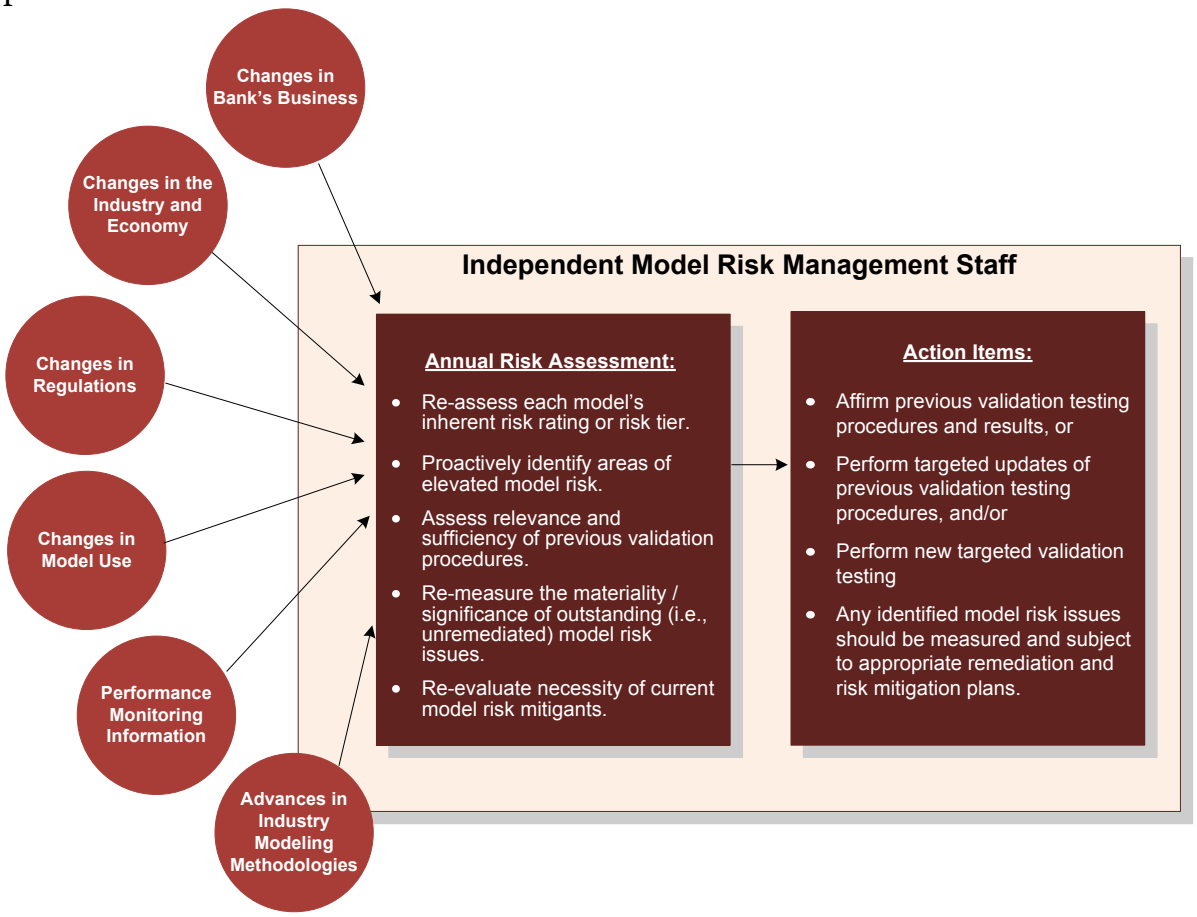
As the Annual Review and On-going Model Risk Monitoring processes are new components of the second-line of defense, we provide further recommendations on these processes below.

[4] Material changes can include changes to the model itself – as well as changes in model use or changes in the inherent risk level of the model.

[5] It is important to distinguish between "model performance monitoring" – which represents regular outcomes analysis such as backtesting and/or benchmarking that is performed by the first line of defense, and "model risk monitoring" which – while inclusive of model performance monitoring – is broader in scope and includes more general types of model-related risks – such as data input risks, model platform risks, etc.

Annual Review Process

The chart below summarizes our views on the primary components of an Annual Review process.



For all models, the Annual Review requires a re-assessment of the model's current inherent risk rating or risk tier.[6] Importantly, models whose risk tier has increased may require performance of additional model validation testing activities that are commensurate with the model's increased risk.[7]

For higher risk models, a great deal more is required of the MRMU – including a re-assessment of current model risk levels related to the actual, or potential, impacts of each of the following:

- Changes in the bank's business policies, practices, products, markets, etc.
- Changes in the industry or economy.
- Changes in external regulations.

[6] It is very common for the MRMU to classify models in the bank inventory according to their perceived degree of inherent risk – with the rigor of model risk management activities varying directly with the assigned risk level. A model's inherent risk level can change over time based on, among other things, changes in model use.

[7] Until such validation testing activities are completed, MRMU and model owner/user should consider designing and implementing an interim risk mitigation plan to address the elevated models risks.

- Changes in model use.
- Results of recent model performance monitoring (e.g., back-testing, benchmarking, sensitivity analyses, and/or stress testing).
- Advances in industry modeling methodologies – for example, improvements in valuation modeling.

For each of these areas, the goal is to evaluate whether residual model risk levels have increased above levels associated with either the last validation cycle or the last Annual Review. For example, if the bank recently entered new geographic markets, then MRMU should consider the impact of this business change to existing higher risk models. Such a change could indicate elevated model risk for certain credit scorecards or other models where geography may be important to the models' performance, and where such models were not developed or validated on data associated with the bank's new geographic markets.

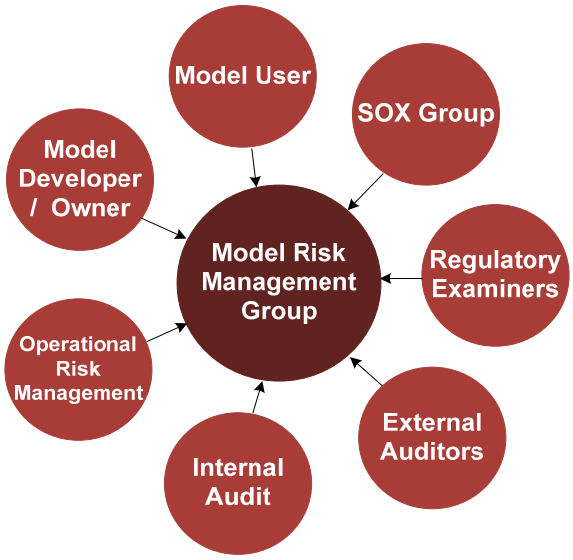
If, based on this assessment, no new emerging risk issues are identified, then the outcome of this risk assessment process would be a re-affirmation of the results of the previous model validation testing and/or Annual Review process. Alternatively, if the assessment identifies one or more emerging risks, then such risks should be measured through the performance of targeted model validation testing activities, and appropriate short-term mitigants and long-term remedial actions should be implemented commensurate with the degree of measured risk.

Other activities that could be part of the Annual Review process are the following:

- *Re-measuring the materiality/significance of outstanding (i.e., un-remediated) model risk issues*. For example, suppose previous model validation testing identified a "bug" in a model's implementation code; however, based on additional testing, it was determined that this bug had an insignificant impact on model results and, therefore, would be remediated at a later date as part of the next model release. Under these circumstances, a re-measurement and re-confirmation of the bug's insignificant impact should be performed regularly until it is fully remediated.
- *Re-confirming required model risk mitigants*. For example, if a model was previously approved under the condition that the first line performs periodic benchmarking of model outputs to third-party estimates, then MRMU should either: (1) re-confirm the continued operation of this risk mitigant, or (2) determine whether the conditions for removal of this mitigant have been satisfied.

On-going Model Risk Monitoring

This process is based on the fact that model-related risks may be identified (directly or indirectly) through other testing activities performed throughout the bank. Accordingly, it is important for such risk information to be collected by, or communicated to, the MRMU to ensure appropriate risk management responses. As the following graphic illustrates, examples of where such information may arise include:



- The model owner/model user – e.g., through first-line model performance monitoring and self-identification of emerging model risk issues.
- Internal Audit – e.g., through business process audits that may identify model-related risks (for example, deficiencies in IT general controls on a system in which one or more models may be deployed).
- The Company's SOX testing group – through periodic testing of internal controls over various financial reporting areas.
- Operational risk management.
- External auditors or regulatory examiners.

Given the potentially wide diffusion of this model risk information throughout the bank, it is important for the MRMU to establish appropriate information linkages to these various groups/areas – whether, for example, through regular meetings, committee participation, or review of issue tracking reports – to ensure effective information collection. Any new model risks identified through this process should be measured by the MRMU through the performance of targeted model validation testing activities, and appropriate short-term mitigants and long-term remedial actions should be implemented commensurate with the degree of measured risk.

Remediation and mitigation of model risk

As discussed above, the MRMU executes three processes to identify and measure model risk on a dynamic, real-time basis: (1) Periodic Model Validation Testing, (2) the Annual Review process, and (3) On-going Model Risk Monitoring. However, these activities represent just the first stage of a larger model risk management process.

Once such risks are identified and measured, the bank must appropriately address them through effective risk mitigation activities. Historically, we note that such risk mitigation activities primarily involved the development of action plans between the MRMU and the model owner that focused on more permanent technical fixes to the model risk issues identified. For example, if a model was exhibiting systematic forecast variances, a typical remediation plan would require the model owner to research the root cause of the model performance deficiency and to develop and implement an associated model change that would address the root cause. Because such "permanent" fixes typically required further

research and development by the model owner, it was common for the MRMU to set relatively long remediation dates for resolution of the identified non-critical risk issues.[8] These remediation plans would then be tracked over time by the MRMU to ensure full remediation of the issues, and senior management – typically through committee structures – would be apprised of remediation status on a consolidated basis.

While this approach, when consistently executed, did achieve the objective of model risk remediation, it also left the bank exposed to elevated model risk levels during the relatively lengthy remediation period. That is, while the 3-12 month long-term action plan was underway, there was no corresponding short-term action plan to mitigate the risk to the bank today based on the model's on-going use(s). Additionally, the MRMU frequently faced difficult decisions of whether to permit model use (i.e., approve the model) in the presence of one or more non-critical model risk issues.

To further evolve the bank's management of model risk, we believe the following risk remediation and mitigation components should be included in the model risk management program:

- *Longer-term action plans focusing on more permanent fixes to the identified model risk issues*. For example, if validation testing revealed a systematic tendency for a model to underpredict actual values by 20%, then a longer-term action plan would be to identify the root cause of the underprediction, and to revise the underlying model accordingly – usually through a re-specification and estimation.[9] However, this type of fix may take several months to complete.
- *Short-term risk mitigants designed to mitigate the risk to the bank today while the long-term fix is being developed*. These mitigants could include, for example, on-top adjustments, on-going benchmarking, model use limitations, or more intensive monitoring of model performance. Continuing our example from above, an appropriate short-term mitigant may be for the model user to implement a 20% on-top adjustment to the model's estimate to offset the measured forecast bias. However, because these short-term mitigants are tied closely with the specific model use(s) (e.g., financial reporting), we believe that it would be inappropriate for the MRMU to be the sole independent approver of these short-term mitigants when the underlying model risks are relatively high.[10]
- It is in this context of short-term risk mitigation of model use that senior management/board governance and oversight of model risk becomes important. This is because an appropriate independent check (or effective challenge) is needed on the model user's proposed short-term mitigant to the identified model risk issue. If, for instance, the model user from our example proposed to the MRMU an on-top adjustment of 10% to mitigate the risk, we are now evaluating two related risks: (1) the original model risk, and (2) a use-specific risk (e.g., material misstatement of valuations, financial reports, market risk measurement, or credit risk measurement). While the MRMU would have a credible opinion on the former, it would typically not be

[8] We also note that it was fairly common for MRMU to defer the implementation of the "permanent" fix to the next version of the model – which also contributed to the lag between the identification of the model risk and its subsequent remediation.

[9] Since long-term action plans are typically focused on the model itself, we believe it is appropriate for the MRMU to have sole authority to approve these (technically-focused) action plans. As noted below, however, we do not believe this would be appropriate for short-term risk mitigants.

[10] It would be inappropriate for the MRMU to make accounting decisions, credit risk decisions, market risk decisions, etc. – each of which can be an important component in determining the appropriate short-term model risk mitigants.

appropriate for the MRMU to make use-specific decisions (e.g., whether a financial estimate is materially accurate or consistent with GAAP/bank accounting policy, whether economic capital levels are appropriate, or whether commercial credit ratings are appropriate).

- For this reason, we believe it is important for proposed short-term mitigants to higher risk model issues to be escalated to appropriate senior management committees for oversight and effective challenge. While escalation could be made to an overall senior management "risk committee", it would be important for this committee to have the right constituency to challenge effectively the different uses that may be escalated. An alternative to a single risk committee would be for certain specialized committees to be designated as escalation points for different model uses (e.g., Asset-Liability Management Committee, Market Risk Committee, Credit Risk Committee, Finance Committee, or Valuation Committee). It is important to note, however, that such oversight and effective challenge is not directly focused on the technical model risk findings; rather, it is focused on whether the model user's proposed short-term mitigation of the model risk is acceptable to senior management and, if applicable, the board.

Final points

There are two additional noteworthy impacts associated with the evolution of bank model risk management frameworks as discussed above:

1. The bank's program is effectively transformed into one that is managed according to residual model risk – a desirable feature from a traditional risk management perspective. Such a framework helps to instill a more formal and effective risk management discipline to the bank that is focused on model risk identification, measurement, remediation and mitigation – and translates it into a common language for senior management and board-level consumption.
2. By focusing on model risk identification, measurement, remediation, and mitigation, this approach eliminates the need to distill the results of model validation testing into a handful of "outcomes" (e.g., Approve, Approve with Minor Qualification, or Not Approved). In our experience, significant time can be spent by the MRMU in determining how to translate the findings arising from its model validation testing into one of these outcomes. At the extreme, we have observed banks create scorecards that assign weights or points to different types of validation findings and, based on the sum of these points, map the validation testing results to one of these outcomes.

   Based on the model risk management framework discussed above, we believe such classifications are both unnecessary and potentially detrimental as they may mask the underlying risk issues identified during model validation testing, the Annual Review process, or through on-going monitoring. Instead of such classifications, the MRMU should focus on the set of risks identified, the measurement of these risks, and how these risks can be mitigated from both a short-term and longer-term perspective. Ultimately, the outcome is not whether the model passes or fails "validation", but whether the identified model risks (and their potential impact on model use(s)) can be effectively mitigated by the model user(s) with appropriate escalation and oversight by senior management (and, where necessary, the board). Put differently, the ultimate goal is whether – with appropriate mitigants – the residual model risks are reduced to an acceptable level consistent with the bank's overall risk appetite.

Additional information

If you would like additional information on Dodd-Frank or about PwC's Financial Services Regulatory Practice, please contact:

Dan Ryan
FS Regulatory Practice Chairman
646 471 8488
daniel.ryan@us.pwc.com

Miles Everson
FS Advisory Practice Leader
646 471 8620
miles.everson@us.pwc.com

Bob Sullivan
Global FS Regulatory Practice Leader
646 471 8388
robert.p.sullivan@us.pwc.com

If you would like additional information about model risk management, please contact:

Ric Pace
703 918 1385
ric.pace@us.pwc.com

Doug Summa
646 471 8596
douglas.summa@us.pwc.com

www.pwc.com/modelrisk

To learn more about financial services regulation from your iPad or iPhone, click here to download PwC's new Regulatory Navigator App from the Apple App Store.

Follow us on Twitter @PwC_US_FinSrvcs

www.pwcregulatory.com