Board of Governors of the Federal Reserve System
Federal Deposit Insurance Corporation
Office of the Comptroller of the Currency

Interagency Statement on Model Risk Management for Bank Systems Supporting Bank Secrecy Act/Anti-Money Laundering Compliance

April 9, 2021

Introduction

The Board of Governors of the Federal Reserve System (Federal Reserve), the Federal Deposit Insurance Corporation (FDIC), and the Office of the Comptroller of the Currency (OCC) (collectively, the agencies), in consultation with the Financial Crimes Enforcement Network and the National Credit Union Administration, are issuing this statement regarding industry questions on model risk management. This statement addresses how the risk management principles described in the agencies' "Supervisory Guidance on Model Risk Management"[1] (referred to as the "model risk management guidance" or MRMG) relate to systems or models used by banks[2] to assist in complying with the requirements of Bank Secrecy Act laws and regulations.

The MRMG (like all supervisory guidance) does not have the force and effect of law. The agencies support efforts by banks to innovate and update their Bank Secrecy Act/Anti-Money Laundering (BSA/AML) systems and models to quickly adapt to an evolving threat environment. The agencies recognize that not all banks use models such as those described in the MRMG for BSA/AML compliance or have formalized model risk management (MRM) frameworks. This statement is intended to clarify how the MRMG may be a useful resource to guide a bank's MRM framework, whether formal or informal, and assist with BSA/AML compliance. Whether a bank characterizes a BSA/AML system (or portions of that system) as a model, a tool, or an application, risk management of such a system should be consistent with safety and soundness principles[3] and the system should promote compliance with applicable laws and regulations.

This statement does not alter existing BSA/AML legal or regulatory requirements, nor does it establish new supervisory expectations. In addition, this statement does not suggest that a bank change existing risk management practices if the bank uses them to effectively manage its risk.

The MRMG is principles-based and articulates the agencies' general views regarding appropriate practices for MRM. It is intended to assist banks that rely on models to do so in a safe and sound

[1] Refer to the "Supervisory Guidance on Model Risk Management," Federal Reserve SR Letter 11-7; OCC Bulletin 2011-12; and FDIC FIL 22-2017.

[2] The term "bank" is used here as in Bank Secrecy Act regulations at 31 CFR 1010.100(d) other than subsection (d)(6). This interagency statement does not apply to credit unions. The term "bank" as used in this interagency statement does include each agent, agency, branch, or office within the United States of banks, savings associations, and foreign banks.

[3] Refer to the "Interagency Guidelines Establishing Standards for Safety and Soundness," 12 CFR 208, Appendix D-1 (Federal Reserve); 12 CFR 364, Appendix A (FDIC); and 12 CFR 30, Appendix A (OCC).

manner, and in compliance with applicable laws and regulations.[4] The MRMG principles provide flexibility for banks in developing, implementing and updating models, including those used for BSA/AML activities. While the MRMG provides a comprehensive discussion of all aspects of model risk management, the practical application of any principle discussed in the MRMG by a bank depends, in part, on the bank's reliance on, and the nature of, its models. While models used for BSA/AML compliance may be different from other models, appropriate model testing and validation processes typically take these differences into account.

Background

Banks routinely use models for a broad range of activities. Models can help to inform and improve business decisions, save money, and reduce the risks that banks face. The use of models can also impose costs, including the potential for unintended and adverse consequences from decisions based on model output that is either incorrect or misused. As reflected in the MRMG, effective model risk management is important because of the potential for poor business and strategic decisions, financial losses, noncompliance with laws and regulations, or damage to a bank's reputation arising from deficient or misapplied models.

Consistent with a risk-based approach, the rigor and sophistication of sound risk management practices are generally commensurate with the bank's overall use of models, the complexity and materiality of its models, and the size and complexity of the bank's operations. If the bank's use of models is less prevalent and has less material impact on the bank's financial condition, operations, or compliance, then a less sophisticated approach to MRM may be appropriate. When models and model outputs could have a material impact on business decisions, including decisions related to risk management, and capital and liquidity planning, and when model failure would have a particularly harmful impact on a bank's financial condition, operations, or compliance, a more extensive and robust MRM framework may be appropriate.

BSA/AML Systems and the MRMG

The agencies' BSA program regulations require a bank to have a reasonably designed compliance program[5] that includes, among its components, a system of internal controls to assure ongoing compliance with BSA regulatory requirements. In this context, effective internal controls are typically based on the bank's risk profile.

BSA/AML systems and a bank's policies, procedures, and processes to identify, research, and report unusual activity, commonly known as suspicious activity monitoring and reporting systems, are critical internal controls for ensuring an effective BSA/AML compliance program. BSA/AML systems may include a surveillance monitoring system, sometimes referred to as an automated transaction monitoring system. Some of these automated transaction monitoring systems may involve the use of modeling.

---

[4] Refer to the "Interagency Statement Clarifying the Role of Supervisory Guidance," issued on September 11, 2018, Federal Reserve Supervision and Regulation Letter 18-5, FDIC Financial Institution Letter (FIL)- 49-2018, OCC News Release 2018-97.

[5] 12 CFR 208.63 (Federal Reserve), 12 CFR 326.8(b) and (c) (FDIC), and 12 CFR 21.21 (OCC), require a bank to establish and maintain a BSA/AML compliance program. *See also* 31 CFR 1020.210 (FinCEN).

There is no definition in statute or regulation of what constitutes a model for the purposes of model risk management; however, the MRMG uses the following definition of a model:

> The term *model* refers to a quantitative method, system, or approach that applies statistical, economic, financial, or mathematical theories, techniques, and assumptions to process input data into quantitative estimates.[6]

The MRMG lists the following three components of a model:

1. An information input component, which delivers assumptions and data to the model.
2. A processing component, which transforms inputs into estimates.
3. A reporting component, which translates the estimates into useful business information.

While some BSA/AML systems may constitute models under this description, others may not. The determination by a bank of whether a BSA/AML system is considered a model is bank-specific, and a conclusion regarding the system's categorization should be based on a consideration of all relevant information. There are no required categorizations of particular BSA/AML systems, including those used to monitor for suspicious activity. Categorizations vary based on the bank's BSA/AML program and the individual features of the bank's BSA/AML systems. The following examples likely would not be considered models, as defined by the MRMG, because they may lack one or more of the three components discussed above:

- Stand-alone, simple tools that flag transactions based on a singular factor, such as reports that identify cash, wire transfer, or other transaction activity over certain value thresholds.
- Systems used to aggregate cash transactions occurring at the bank's branches for the purposes of filing Currency Transaction Reports.

Regardless of whether a bank characterizes a BSA/AML system as a model, a tool, or an application, there is no specific organizational structure required for oversight by the bank. Oversight of BSA/AML systems might be conducted solely by the bank's compliance area, an MRM group, another functional area, or some combination of these functions. Sound risk management and procedures for evaluating the effectiveness of compliance programs are both key components to an effective BSA/AML compliance program.

The MRMG is nonbinding and provides principles that may be helpful in managing the BSA/AML compliance program. There is no requirement or supervisory expectation that banks have duplicative processes for complying with BSA/AML regulatory requirements. For automated transaction monitoring systems, prudent risk management involves periodically[7] reviewing and testing the filtering criteria and thresholds to ensure that they are still effective, as

---

[6] The definition of "model", as described in the MRMG, also covers quantitative approaches whose inputs are partially or wholly qualitative or based on expert judgment, provided that the output is quantitative in nature.

[7] Model reviews and validations are generally performed using a risk-based approach, and with a frequency appropriate for (or when there are changes to) a bank's risk profile. BSA/AML risk profile changes may include new or revised bank products, services, customer types, or geographic locations, or if the bank expands through mergers and acquisitions. Material changes to models likely warrant validation.

well as independently validating the monitoring system's methodology and effectiveness to ensure that the monitoring system is detecting potentially suspicious activity.

Further, there is no requirement that a bank perform duplicative independent testing activities, including model validation, to ensure compliance with BSA/AML regulations. In certain cases, validation conducted on models may help a bank in its independent testing for BSA/AML purposes; similarly, some aspects of independent testing for BSA/AML purposes may assist a bank in its model validation activities. Generally, the principles for risk management set forth in the MRMG provide a framework that can be used to help support an effective BSA compliance program.

Model risk management includes disciplined and knowledgeable development and implementation processes that are consistent with the situation and goals of the model user and with bank policy.[8] In the context of BSA/AML systems that are considered by a bank to be models, sound model development and validation activities typically align with the purpose of each model and incorporate model objectives, structure, data, methodologies, complexity, and extent of use. The extent and nature of model risk varies across models and banks, and a bank's risk management framework is most appropriately tailored when it is commensurate with the nature and materiality of the risk. For example, a bank's MRM framework may support the implementation of less material changes to models without revalidation, or with the revalidation of certain model components without revalidating the entire model, in appropriate circumstances. Overall, the statements contained within the MRMG are meant to provide useful information for the bank's consideration and are not to be regarded as "templates" or requirements.

The MRMG describes how banks may objectively assess model risk using a sound model validation process, including evaluation of conceptual soundness, ongoing monitoring, and outcomes analysis. A central principle for managing model risk is "effective challenge" of models, which refers to critical analysis by objective, informed parties. For banks that use models to comply with the BSA/AML requirements, it is important that validation be performed by individuals with sufficient expertise and an appropriate level of independence from the model's development and implementation. An appropriate level of independence for individuals performing model validation is also important when banks outsource multiple functions to the same third party.

The agencies recognize that the objectives and structure of BSA/AML models (BSA/AML systems determined by a bank to be models) may differ from those in other business units because the objectives of most BSA/AML models place greater emphasis on coverage over efficiency. BSA/AML models may require quick adjustments to reflect the changing nature of criminal behavior or the bank's risk profile. Similarly, testing and performance monitoring for some BSA/AML models may not include the same techniques as other models because of various factors, such as the lack of information about realized outcomes (e.g., Suspicious Activity Reports). The MRMG notes that the nature of testing and model assessment can vary across models and recognizes that for some models complete information may not be available. A bank's validation methodology may take such differences into account. For example, a bank

[8] The systems, processes, models, or tools used by a bank for BSA/AML purposes must be consistent with relevant laws and regulations.

may choose to accept a reduction in efficiency (such as by producing more alerts) in exchange for greater coverage in its automated transaction monitoring system. Banks typically make these decisions based on risk and change or update controls, as appropriate, to ensure that effective controls are in place.

Third-Party Models

Third-party models can assist banks in improving the efficacy of their BSA/AML programs, and reasonable due diligence prior to entering into a contractual relationship with a third party is important to a successful relationship. In addition, ongoing monitoring of the third party and the model is important when a bank depends on a third-party model for compliance-related activities, such as currency transaction reporting, monitoring transactions, detection of suspicious activity, or suspicious activity reporting.

Banks are ultimately responsible for complying with BSA/AML requirements, even if they choose to use third-party models to assist with their BSA/AML compliance programs. In doing so, banks may consider the principles discussed in the agencies' third-party risk management issuances and the aspects of the MRMG that address third-party models.[9] Although the proprietary nature of third-party models is a consideration, sound risk management practices include obtaining sufficient information from the third party to understand how the model operates and performs, ensuring that it is working as expected, and tailoring its use to the unique risk profile of the bank. These practices assist in meeting BSA/AML regulatory compliance requirements.[10]

An understanding of how the third-party model operates is important to the bank's ability to effectively negotiate contracts that will protect the bank's needs and rights, including needs and rights concerning privacy and information security. In addition, it is important that banks using third-party models have contingency plans if the third-party model is no longer available or serviced or may no longer be reliable.

Conclusion

In summary, the extent and nature of model risk varies across models and banks, and effective risk management is commensurate with the nature and materiality of the risk. The agencies are clarifying, in this statement, the following points:

- The MRMG, like all supervisory guidance, does not have the force and effect of law. Banks may use some or all of the principles in the MRMG in their risk management processes to support meeting the regulatory requirements of an effective BSA/AML compliance program. Banks with limited model use may not have formal MRM frameworks.

---

[9] Refer to OCC Bulletin 2013-29, "Third-Party Relationships: Risk Management Guidance" (OCC), OCC Bulletin 2020-10, "Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29" (OCC); SR 13-19 (Federal Reserve); and FDIC FIL-44-2008, "Guidance for Managing Third-Party Risk" for more information regarding third-party risk management.

[10] Refer to the agencies' third-party risk management issuances noted in footnote 8 and the discussion of third-party models in the MRMG for more information.

- The MRMG is not meant to serve as a set of testing procedures, including with regard to BSA/AML systems.

- The MRMG does not establish any requirements or supervisory expectations that banks have duplicative processes for complying with BSA/AML regulatory requirements.

- Certain processes and systems used in BSA/AML compliance may not be models. The determination by a bank of whether a system used for BSA/AML compliance is considered a model is bank-specific. When making this determination, a bank may consider the MRMG model definition and the three components that characterize models.

- Banks assess different models in different ways. The nature of testing and analysis of models depends on the type of model and the context in which the models are used.

- The MRMG principles provide flexibility for banks in developing, implementing, and updating models. Banks may benefit from employing this flexibility, including for validation activities, to update BSA/AML models quickly in response to the evolving threat environment and to implement innovative approaches. Banks may establish policies that govern when the bank may implement less material changes to models without revalidation, or may choose to revalidate certain model components without revalidating the entire model.

- Banks may choose to use a third-party model. When doing so, banks may consider the principles discussed in the agencies' third-party risk management issuances and the aspects of the MRMG that address third-party models.

- Regardless of how a BSA/AML system is characterized, sound risk management is important, and banks may use the principles discussed in the MRMG to establish, implement, and maintain their risk management framework.