Prepared for: Federal Deposit Insurance Corporation

Re: Request for Information on Standard Setting and Voluntary Certification for Models and Third-Party Providers of Technology and Other Services RIN 3064-ZA18

Prepared by:
First Midwest Bank
Emmanuel Salta
Model Risk Analyst
Emmanuel.Salta@firstmidwest.com
8750 W. Bryn Mawr Avenue, Suite 1300
Chicago, IL 60631

https://www.govinfo.gov/content/pkg/FR-2020-07-24/pdf/2020-16058.pdf

General

Question 1: Are there currently operational, economic, marketplace, technological, regulatory, supervisory, or other factors that inhibit the adoption of technological innovations, or on-boarding of third parties that provide technology and other services, by insured depository institutions (IDIs), particularly by community banks?

Question 2: What are the advantages and disadvantages of establishing standard- setting and voluntary certification processes for either models or third-party providers?

Advantages: For models, I would expect that the standard-setting and voluntary certification processes would at least confirm the evaluation of conceptual soundness portion of the model validation requirements. This, however, would not certify the proper use of the model specific to a bank. Testing of the model using the bank's data and outputs would still be required in the model validation.

Question 3: What are the advantages and disadvantages to providers of models of participating in the standard-setting and voluntary certification process? What are the advantages and disadvantages to providers of technology and other services that support the IDI's financial and banking activities of participating in the standard-setting and voluntary certification process?

Advantages: With a certification or seal of approval, model providers would have an easier time promoting their models to banking institutions.

Disadvantages: During the certification process, model providers might be required to reveal their proprietary codes to certifiers thus losing their potential competitive advantage in the marketplace. Vendors might compensate by charging higher fees compared to non-certified models.

Question 4: What are the advantages and disadvantages to an IDI, particularly a community bank, of participating in the standard-setting and voluntary certification process?

Advantage: Process might lower model risk from the IDI end.

Disadvantage:

Question 5: Are there specific challenges related to an IDI's relationships with third-party providers of models or providers of technology and other services that could be addressed through standard-setting and voluntary certification processes for such third parties?

1) **Are there specific challenges related to due diligence and ongoing monitoring of such third-party providers?**

   The process could potentially shorten the time period of conducting due diligence of third-party providers.

2) **Are there specific challenges related to the review and validation of models provided by such third parties?**

   The review and validation of third-party models using the standard-setting process will most likely not cover the individual bank's usage of the model, in particular the ongoing performance assessment unique to the bank's data.

3) **Are there specific challenges related to information sharing or data protection?**

Question 6: Would a voluntary certification process for certain model technologies or third-party providers of technology and other services meaningfully reduce the cost of due diligence and on-boarding for: (1) the certified third-party provider? NA **(2) the certified technology?** Depends on the technology. New technologies would probably increase the cost seeing that there

are no standards readily available for them. **(3) potential IDI technology users, particularly community banks?** Same answer as (2).

Question 7: What are the challenges, costs, and benefits of a voluntary certification program or other standardized approach to due diligence for third-party providers of technology and other services? How should the costs of operating the SSO and any associated COs be allocated (e.g., member fees for SSO participation, certification fees)?

Question 8: Would a voluntary certification process undermine innovation by effectively limiting an IDI's discretion regarding models or third-party providers of technology and other services, even if the use of certified third parties or models was not required? Would IDIs feel constrained to enter into relationships for the provision of models or services with only those third parties that are certified, even if the IDIs retained the flexibility to use third parties or models that were not certified?

I don't the IDI would feel constrained. A balance between the bank's need for that particular model and the cost are the drivers in the decision to

Question 9: What supervisory changes in the process of examining IDIs for safety and soundness or consumer protection would be necessary to encourage or facilitate the development of a certification program for models or third-party providers and an IDI's use of such a program? Are there alternative approaches that would encourage or facilitate IDIs to use such programs?

There should be clear language regarding the process of examining IDIs that use certified models. In using a certified model, an IDI should only be responsible for a limited scope validation, e.g., its use of the model.

Question 10: What other supervisory, regulatory, or outreach efforts could the FDIC undertake to support the financial services industry's development and usage of a standardized approach to the assessment of models or the due diligence of third-party providers of technology and other services?

Make full certification report available to IDIs.

Scope

Question 11: For which types of models, if any, should standards be established and a voluntary certification process be developed? For example, is the greatest interest or need with respect to: (1) traditional quantitative models? (2) anti-money laundering (AML) transaction monitoring models? (3) customer service models? (4) business development models? (5) underwriting models? (6) fraud models? (7) other models? or need with respect to: (1) traditional quantitative models? (2) anti-money laundering (AML) transaction monitoring models? (3) customer service models? (4) business development models? (5) underwriting models? (6) fraud models? (7) other models?

Give priority in certifying models that use newer techniques but are widely used., e.g., machine learning/AI applications to AML models.

Question 12: Which technical and operational aspects of a model would be most appropriate for evaluation in a voluntary certification program?

Question 13: What are the potential challenges or benefits to a voluntary certification program with respect to models that rely on artificial intelligence, machine learning, or big data processing?

Benefit to IDI - Better transparency in the use of modeling techniques mentioned.

Question 14: How can the FDIC identify those types of technology or other services, or those aspects of the third-party provider's condition, that are best suited for a voluntary certification program or other standardized approach to due diligence? For example, should such a certification program include an assessment of financial condition, cyber security, operational resilience, or some other aspect of a third-party provider?

Create a working group composed of SMEs from universities and industry.

SSO

Question 15: If the FDIC partnered with an SSO to set standards for due diligence and assessments of models or third-party providers of technology and

other services, what considerations should be made in choosing the SSO? What benefits or challenges would the introduction of an SSO into the standard-setting process provide to IDIs, third- party providers, or consumers?

Who will set the standards for choosing the SSO? What will those standards be?

Question 16: To what extent would a standards-based approach for models or third-party providers of technology and other services be effective in an environment with rapidly developing technology systems, products, and platforms, especially given the potential need to reassess and reevaluate such systems, products, and platforms as technologies or circumstances change?

For banks that don't have the resources to maintain a technical team, the certification process would at least provide them with confidence that they are using reliable certified models.

Question 17: What current or draft industry standards or frameworks could serve as a basis for a standard-setting and voluntary certification program? What are the advantages and disadvantages of such standards or frameworks? Do standards and voluntary certifications already exist for use as described herein?

Question 18: Given that adherence to SSO standards would be voluntary for third parties and for IDIs, what is the likelihood that third-party providers of models or services would acknowledge, support, and cooperate with an SSO in developing the standards necessary for the program? What challenges would hinder participation in that process? What method or approaches could be used to address those challenges?

Depends on the incentive given to third-party providers and the available market for certified models.

Question 19: What is the best way to structure an SSO (e.g., board, management, membership)? Alternatively, are there currently established SSOs with the expertise to set standards for models and third parties as described herein?

Question 20: To what extent should the FDIC and other federal/state regulators play a role, if any, in an SSO? Should the FDIC and other federal/state regulators provide recommendations to an SSO? Should the FDIC and other federal/state regulators provide oversight of an SSO, or should another entity provide such oversight?

Certification Organizations (COs)

Question 21: What benefits and risks would COs provide to IDIs, third parties, and consumers?

Question 22: To what extent would COs be effective in assessing compliance with applicable standards in an environment with rapidly developing technology systems, products, and platforms, especially given the potential need to reassess and reevaluate such systems, products, and platforms as technologies or circumstances change?

Question 23: For model validation and testing, would COs evaluate a model based solely on reports, testing results, and other data provided by the third-party provider of the model? Or would the COs need to test the model and generate their own test results? What steps would the COs need to take to protect the intellectual property or other sensitive business data of the third party that has submitted its model to the validation process?

CO should be able to reproduce the results provided by the third-party provider preferably using a different approach. If any other tests are needed, the CO should be able to perform such tests.

Question 24: If COs receives derogatory information indicating that a certified third party or certified model or technology no longer meets applicable standards, should the COs develop a process for withdrawing a certification or reassessing the certification? (1) If so, what appeal rights should be available to the affected third party? (2) What notification requirements should COs have for financial institutions that have relied on a certification that was

subsequently withdrawn? (3) Should the FDIC or federal/state regulators enter information sharing agreements with COs to ensure that any derogatory information related to a certified third party or certified model or technology is appropriately shared with the COs?

Question 25: Are there legal impediments, including issues related to liability or indemnification, to the implementation of a voluntary certification program that the FDIC, other federal/state regulators, third-party providers, and IDIs should consider?

Question 26: To what extent should the FDIC and other federal/state regulators play a role, if any, in the identification and oversight of COs, including assessments of ongoing operations? Should the FDIC and other federal/state regulators provide oversight of COs, or should another entity, such as an SSO, provide such oversight?